Cisco Remote Expert Mobile Version 11.5(1)

Installation and Configuration Guide

First Published: 2016-08-10
Last Modified: 2016-12-15

Preface

Change History

Changes	Date
Initial release	2016-08-10
Updated Features section detailing co-browse only features	2016-10-31
Updated throughout to signal which features are not relevant for co-browse only version	
New section for Testing with Co-browse Only added	2016-11-23

About This Guide

This document outlines the steps necessary to install and configure Cisco Remote Expert Mobile (RE Mobile) Open Virtual Appliance (OVA). This deployment guide specifies:

- The VM platform requirements for Remote Expert Mobile
- How to load the Remote Expert Mobile `.ova` installation file
- How to install and configure Remote Expert Mobile in different topologies

Prior to Install and Configuration, you should read and be familiar with *Cisco Remote Expert Mobile—Design Guide*.

If you require VMware infrastructure training, you must acquire the necessary knowledge and experience regarding deployment and management of virtual machines before you deploy components on VMware virtual machines.

This guide assumes that you are familiar with basic contact center and unified communications terms and concepts. This guide provides the required DNS, NAT, reverse proxy and firewall configuration information but 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 and brief overview of Remote Expert Mobile and its SDKs, software server components, agent integrations and key technologies.
Overview of Remote Expert Mobile Deployment Options	Describes the standard Remote Expert Mobile deployment models: single box, all-in-one deployment and highly available multi-box clustered deployment for the RE Mobile OVA
Before You Begin	Lists Infrastructure requirements
Installing RE Mobile for a Single Master Node / All-In-One Deployment	Table showing sequence of operations required to install RE Mobile for a single-node deployment.
Installing the Base Multi-node HA Deployment	Table showing sequence of operations required to install RE Mobile for a multi-node deployment.
Install and Configure the Virtual Machine(s)	Describes hardware, software and configuration requirements for the virtual machine(s) needed to run RE Mobile
Configure the NTP Service	Describes the procedure for configuring the NTP service
Configure the HTTP Reverse Proxy	Describes the configuration of the reverse proxy needed for RE Mobile
Configure the Domain Name Service (DNS)	Describes the procedure for configuring the DNS service
Install the Remote Expert Mobile OVA	Describes the procedure for installing the REM OVA. Includes subsections for Single- and Multi-node deployments.
Configuration and use of Transport Layer Security (TLS) in REAS	Ensure successful installation of TLS certificates
Operating System	Describes how to gain access to the hosts' operating systems
Remote Expert Mobile Administration Console	Describes how to access the REM Administration Console
Expert Assist Configuration—Consumer Access Number Regex	Configuration of destination number restriction by regular expression.
Expert Assist Configuration—Image Quality Scale Factor	Configuration of screen share quality using Expert Assist
Post Install Verification	Perform test calls and Expert Assist sessions
Integrating Remote Expert Mobile	Ensure successful RE Mobile integration with your UC or CC environment
Restricting Application URIs via the Reverse Proxy	List of the URIs that should be allowed through the Reverse Proxy
Additional Information	VMware specifics
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 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-browse and application sharing in mobile or web applications. Cisco Remote Expert Mobile is designed specifically for remote collaboration services provided through Cisco Unified Communications Manager, Cisco Unified Contact Center Enterprise (Unified CCE) and / or Cisco Unified Contact Center Express (Unified CCX). Remote Expert Mobile offers the following features and options that are pre-sized within core components. Core component features are:

- In-app voice and video communications (Over-the-Top WebRTC communications)
  - High definition video and audio
  - Bi-directional or one-way video
  - Mute audio, video or both
  - Client side call control
- WebRTC to SIP gateway (trunking into Cisco Unified Border Element and Unified Communications Manager)
- Expert Assist
  - Web co-browse
  - 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
- 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 and G.729a audio transcoding into the enterprise network
  - H.264 and VP8 video transcoding

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)

SDKs

Cisco Remote Expert Mobile includes Software Development Kits (SDKs). In the full edition, they provide voice over IP, video over IP, and Expert Assist (app share and web co-browse, annotation and document push) features within pre-existing mobile and web applications.

RE Mobile's Client SDK for Web supports every major browser such as:

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

In browsers which support WebRTC, the full edition of Remote Expert Mobile provides 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 and Expert Assist features in iOS and Android apps through native libraries.

When used with the co-browse only edition, the same SDKs supply the Expert Assist functionality (application sharing and co-browse, annotation and document push) without the need for plugins.

Overview of Expert Mobile Deployment Options

As detailed in *Cisco Remote Expert Mobile—Design Guide*, the RE Mobile OVA may be used to install RE Mobile two configurations: single-node or multi-node configuration.

1. Single Node, all-in-one deployment
   - All services (Remote Expert Application Server (REAS) and Media Broker (REMB)) deployed to a single Virtual Machine (VM).
   - This is ideal for development test-beds, proof of concept and small-scale deployments.
2. Base HA Multi-node deployment
   - This deployment model is made up of multiple VMs, each hosting either an REAS or a REMB.
   - A multi-box topology would typically be used for production deployments.

Note: The OVA is used to create a VM hosting the REAS (which hosts the Web Gateway, Expert Assist as well as the Finesse Gadgets and Expert Assist Web Consoles) and/or the REMB. The same OVA template file is used to deploy RE Mobile in any required topology.

These deployment scenarios cover the integration of CUBE, UCCE, CUCM, and CCX. This guide does not cover Remote Expert Mobile deployed exclusively with Unified CM.

Note: For Remote Expert Co-browse, the REMB is not needed. Only the HTTP/WSS messages will be used. Instructions which refer to installing a REMB can be ignored.

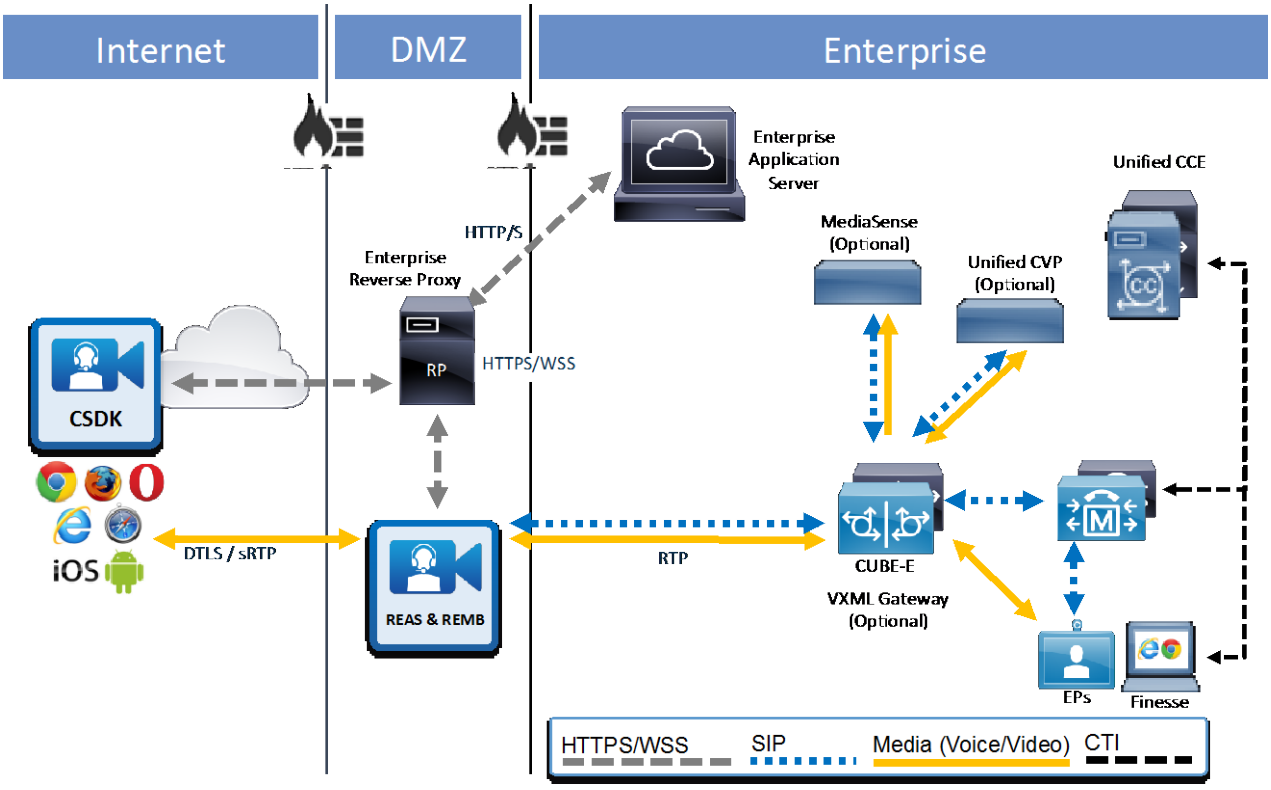
Single Node, All-In-One Topology

Using the OVA template, Remote Expert Mobile can easily be setup as a single master VM with both REAS and REMB service running concurrently.

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

The role of the reverse proxy within this deployment is described in the Functions of the HTTP Reverse Proxy section below.

Figure 1. Single Node Topology



Functions of the HTTP Reverse Proxy

A reverse proxy is a type of proxy server that retrieves resources on behalf of a client from one or more servers—these resources are then returned to the client as though they originated from the proxy server itself.

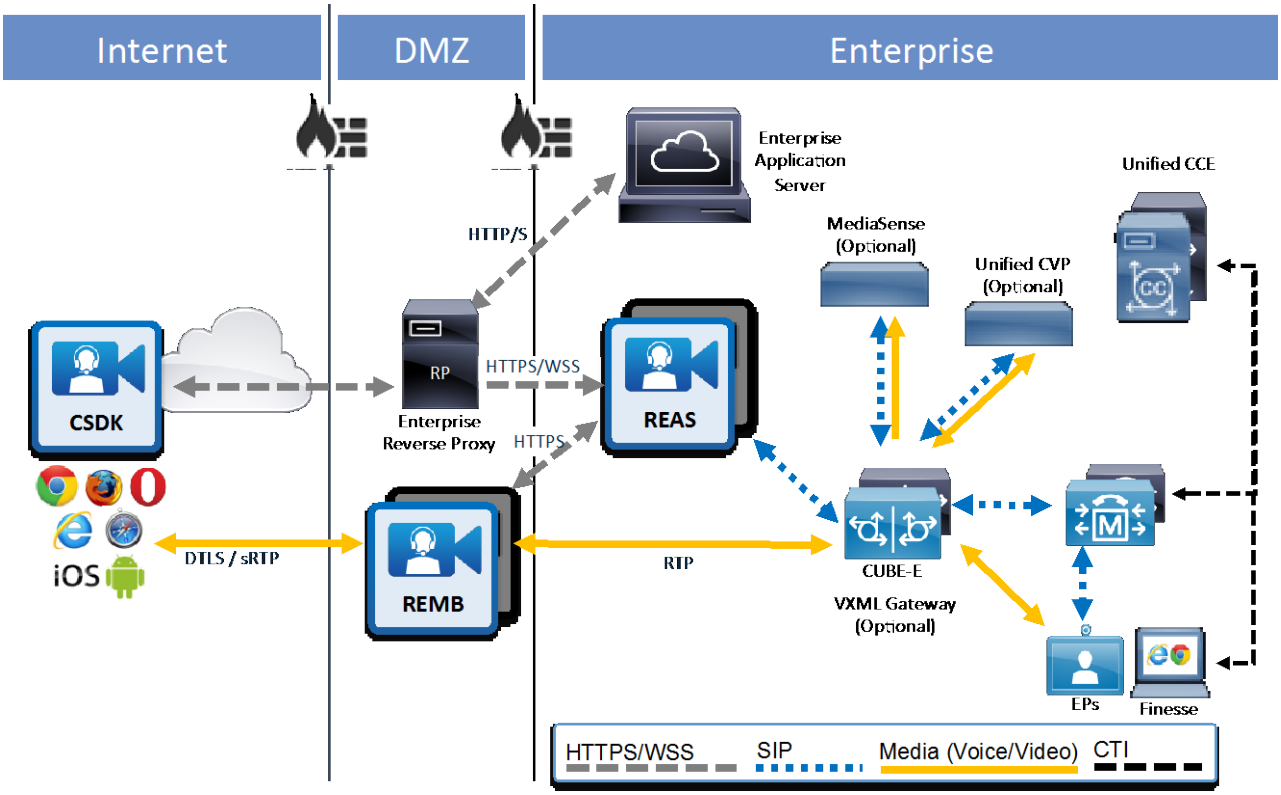
Multi-node, Clustered Topology

Remote Expert Mobile **Base HA Multi-node Deployment** is a four (4) node cluster (2 REAS and 2 REMB).

This is a minimum setup for a High Availability (HA) configuration—as such, it can support up to 100 concurrent video, audio and expert sessions; that is, there is redundancy if an REAS or REMB fails, and a single REMB can support up to 100 sessions.

> **Note:** Every Remote Expert Mobile Application Server cluster must consist of a single master node, and from 1 – 9 slave nodes. The master node must be created prior to slave nodes being created.
>
> For the base multi-node HA deployment, there are two REAS servers, one master and one slave; in a bigger multi-node HA deployment, there will be more than 2 REAS nodes.
>
> The role of the reverse proxy within this deployment is described in the Functions of the HTTP Reverse Proxy section on page 9.

Figure 2. Base HA Multi-node Deployment



Before You Begin

Infrastructure Requirements

Supporting infrastructure must be in place before beginning to deploy and configure RE Mobile. This infrastructure will consist of the following:

- A suitable virtual machine
- Proper NTP configuration
- Proper HTTP Reverse Proxy configuration
- Proper DNS configuration
- Ensure that Multicast is enabled between Master & Slave REAS servers (not required for Media Brokers)
- If you intend to enable MOWS (Media-over-WebSockets), consider the implications of the potential extra traffic on your existing infrastructure.

REM Users and Security

The Operating System shipped with Remote Expert Mobile 10.6 included only a root user, which was used to run the Remote Expert Mobile processes, to gain SSH access and to execute all command-line actions. Having all activities occurring under a single user with root access creates security concerns for the system.

In order to mitigate many of the security concerns we have introduced additional users for Remote Expert Mobile 11.5(1). There are three new users, the default user names are as follows:

- **REM OS User (rem-user)**—operates REM, for example starts and stops REAS and REMB
  The Remote Expert Mobile services are executed as this user and it has the following permissions:
  - Write and execute permissions limited to files/directories where it is required
  - SSH access is disabled for this account.
- **REM OS Admin User (rem-admin)**—performs upgrades and any other administrator-level tasks
  This account has all permissions associated with **rem-user**, with the addition of the following:
  - Able to execute the REM upgrade procedure and the log capture scripts with elevated permissions
  - Able to execute any REM-related scripts
  - SSH access is disabled for this account.
- **SSH OS User (rem-ssh)**—the only user allowed to SSH into the box
  This account allows SSH access, with the following constraints:
  - It is limited in its abilities
  - It is only used to switch to one of the other operating system accounts.

In addition to the above users, SSH access is disallowed for the root user.

The `setup.sh` script prompts for these users (see Running The Setup Script on page 28), as does the upgrade. (see Upgrade Procedure on page 86).

Considerations

The following considerations apply after these changes:

- The root user is only present in case there is an unexpected administrative task that needs to be performed—in normal maintenance of the system no-one needs to log in as the root user.
- The system processes run as a user with reduced permissions. Specifically, the user's execute and write permissions are now restricted to necessary locations, so that if a Remote Expert Mobile system were to be compromised through the running processes, the effects on OS security would be minimal.
- OS-level maintenance and administration, including system upgrade, are run as a user with restricted permissions. Elevated permissions are granted only for the specific scripts that require them, meaning that a user logged in with this account could not accidentally run a dangerous command on the Remote Expert Mobile machine.
- The account that allows remote access does not have permission to do anything malicious to the machine, meaning that a malicious user would need at least 2 passwords in order to seriously compromise system security.

Security information

The OVA installation sets up self-signed certificates—after installation is complete, we expect and encourage you to replace these with certificates signed by a CA, and to change the default KeyStore/TrustStore passwords.
See Changing Passwords on page 53.

Installing RE Mobile for a Single Master Node / All-In-One Deployment

The sequence of procedures for installing RE Mobile for a Single Master Node / All-in-one deployment are shown in the table below:

Sequence	✓	Task	Notes
1		Install and configure the virtual host	See Install and Configure the Virtual Host(s) on page 15
2		Configure NTP	See Configure the NTP Service on page 16
3		Install and configure the HTTP Reverse Proxy	See Configure the HTTP Reverse Proxy on page 17
4		Install and configure DNS	See Configure the Domain Name Service (DNS) on page 17
5		Deploy the OVA for Single Master Node / All-In-One deployment	See Installing a Single Master Node / All-In-One Deployment on page 18
6		Verify the installation	See Post-Install Verification on page 50
7		Configure Transport Layer Security in REAS	See Configuration and use of Transport Layer Security (TLS) in REAS on page 34
8		Log into the host's operating system	See Operating System on page 41
9		Use a browser to access the Remote Mobile Administration Console	See Remote Expert Mobile Web Administration Console on page 42
10		Configure Remote Expert Assist	See Expert Assist Configuration—Consumer Access Number Regex on page 46
11		Integrating RE Mobile into a Contact Center Environment	See Integrating RE Mobile into a Contact Center Environment on page 64
12		Test the Agent Console	See Testing the CC Integration on page 68
13		Restrict Application Via the Reverse Proxy	See Restricting Application URIs via the Reverse Proxy on page 69

Installing the Base Multi-node HA Deployment

The sequence of procedures for installing RE Mobile for a Single Master Node / All-on-one deployment are shown in the table below:

Sequence	✓	Task	Notes
1		Install and configure the virtual host	See Install and Configure the Virtual Host(s) on page 15
2		Configure NTP	See Configure the NTP Service on page 16
3		Install and configure the HTTP Reverse Proxy	See Configure the HTTP Reverse Proxy on page 17
4		Install and configure DNS	See Configure the Domain Name Service (DNS) on page 17
5		Deploy the OVA for Base Multi-node HA deployment	See Installing a Base Multi-node HA Deployment on page 20
6		Install and Configure the REMB for Base Multi-node HA deployment	See Installing and Configuring a REMB (Base Multi-node HA deployment) on page 23 **Note**: Ignore this step in co-browse only edition
7		Verify the installation	See Post-Install Verification on page 50
8		Configure the Transport Layer Security (TLS) in REAS	See Configuration and use of Transport Layer Security (TLS) in REAS on page 34
9		Log into the host's operating system	See Operating System on page 41
10		Use a browser to access the Remote Mobile Administration Console	See Remote Expert Mobile Web Administration Console on page 42
11		Configure Remote Expert Assist	See REMB Settings in UCCE, UCCX, and UC Environments on page 44
12		Integrating RE Mobile into a contact center environment	See Integrating RE Mobile into a Contact Center Environment on page 64
13		Test the Agent Console Gadgets	See Testing the CC Integration on page 68
14		Configure the Reverse Proxy to restrict the application URIs	See Restricting Application URIs via the Reverse Proxy on page 69

Install and Configure the Virtual Host(s)

This section lists the recommended platform and specifications-based system requirements. The requirements outlined refer to the minimum requirements for a VM host to support RE Mobile. The minimum requirements for future releases may differ, and you should refer to the following guides to ensure that pre-requisites are met:

- *Cisco Remote Expert Mobile—Design Guide* > VM Specifications and Constraints
- *Cisco Remote Expert Mobile—Release Notes*

You will require a separate VMware host for each RE Mobile node you intend to provision. For an all-in-one single box deployment, you will only require a single VMware host. For a multi-box installation, you will need multiple hosts available.

Hardware and system Requirements

RE Mobile requires a server platform that meets VMware's Compatibility Guide for VMware vSphere 5.x or later. 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 specifications for supported platforms.

Each RE Mobile node is deployed as a virtual server and requires a VMware server to act its host. The server operating system is CentOS. RE Mobile is an on-premises deployment. All services are set up, managed, and maintained on your corporate network.

Note: When configuring the hosts networking settings, the administrator should configure vswitch/port groups to support the deployment type. A single master node guest vm typically requires one interface (external) to be mapped, whereas the multi node master guest typically requires 2 or 3 interfaces (external, internal, management) to be mapped.

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"

Prior to installing the RE Mobile OVA, ensure that you have a suitable vCenter environment prepared. This environment will consist of a VMware vSphere Datacenter and a VMware host. (Refer to the OVA Deployment section below for information that will help you to calculate the proper resource allocation for your VMware host(s).)

Note: For more information on installing and configuring VMware Sphere and hosts, see the VMware documentation at https://www.vmware.com/support/pubs/

Remote Expert Mobile is delivered as an OVA image, and deployed as described in this document.

Configure the NTP Service

Ensure that the VMware host is configured with a valid NTP server—the same NTP server that will be specified in Expressway.

Procedure

Step 1	Select the host.
Step 2	Go to the **Configuration** tab.
Step 3	Select Time configuration.
Step 4	Select Properties.
Step 5	If the date and time were red on the previous page, set the date and time manually to the current time.
Step 6	Click Options.
Step 7	Select NTP Settings and click Add.
Step 8	Enter the IP address of the NTP server and click **OK**.
Step 9	Select Restart NTP service to apply changes check box
Step 10	Click **OK** … and Click **OK** again

Configure the HTTP Reverse Proxy

The HTTP Reverse Proxy must be installed in front of the REAS in the DMZ. Supported Reverse Proxies include the following:

- Apache
- F5
- Nginx.

For information on configuring HTTP Reverse Proxy, see the documentation for the specific Reverse Proxy that you are using.

Configure the Domain Name Service (DNS)

RE Mobile requires DNS when installing a multi-box environment. The following is a list of the required DNS entries.

- An FQDN for each REAS VM (for example, server-A.example.com, server-B.example.com, etc.
- A cluster address (also known as a service address). This is a single FQDN that resolves to all the REAS nodes. This is the FQDN that the cluster as a whole is contactable on.

Note: For more information on configuring DNS, see the documentation for your particular DNS server.

Install the Remote Expert Mobile OVA

General

This section outlines installation for the following RE Mobile deployment topologies.

1. **Single master node**—an all-in-one deployment for testing and development use
2. **Base HA Multi-node**—a clustered deployment for production use

Cisco RE Mobile software is flexible in its support of multiple deployment options. Running in a virtualized environment, enterprises can run RE Mobile on any hardware platform that meets the specifications outlined above. This makes it easy to manage and deploy RE Mobile within an existing data center.

Along with the CentOS operating system and Oracle Java, the OVA template includes the following:

- The RE Mobile Application Server (REAS),
- Remote Expert Mobile Client SDKs (CSDK)
- Expert Assist Web Agent and Supervisor Consoles
- Expert Assist Agent and Supervisor Consoles
- Remote Expert Mobile Media Broker (REMB)

Note: Before undertaking an installation of the Cisco RE Mobile OVA, be sure to review the *Cisco Remote Expert Mobile—Design Guide*.

Note: REMB nodes are not needed for Remote Expert Co-browse

Installing a Single Master Node / All-In-One Deployment

The steps below describe how to use an OVA to deploy the simplest RE Mobile configuration. It results in a single VM guest that contains both REAS and REMB components.

Note: Single master node deployments should only be used for non-critical development or lab systems.

Interface Selection

The single-node deployment has only one REAS and one REMB within its cluster. When deploying the OVA as a single box, all-in-one topology, the simplest and recommended configuration is to define only the “External” interface.

OVA Deployment

Step 1: Download the RE Mobile OVA through your usual distribution channels.

Note: The OVA is a large file—allow sufficient time to download the OVA prior to beginning an installation.

Step 2: Launch the VMware vSphere client on your local machine and connect to your vCenter Server.

Step 3: Select the VMware Datacenter containing the VMware host you intend to deploy to.

Step 4: Click: File > Deploy OVF Template…

Step 5: Browse to locate the RE Mobile OVA file. Click **Next**.

Step 6: Review OVF image details and click **Next** to continue.

Step 7: Click **Accept** for each license agreement. When all license agreements have been accepted, click **Next.**

Step 8: Specify a name and location for the deployed template. Choose the VMware Datacenter containing the VMware host you intend to deploy into and click **Next**.

Note:
– The specific VMware host will be selected in a later step.
– We recommend that you change the VM guest name to something more descriptive, for example REAS-MASTER or REAS-SLAVE.

Step 9: Select the desired hardware deployment configuration.

The deployment template enables you to choose from one of the following VM *hardware* configurations—Small Machine, Singlebox (Developer), or Large Machine.

Note that this is different from the option of what software you wish to deploy.

a. Remote Expert Mobile—Small Machine

Requires 4 vCPU (8400 MHz reservation) and 4 GB RAM (4 GB reservation)

b. Remote Expert Mobile—Singlebox (Developer)

Requires 4 vCPU (8400 MHz reservation) and 6 GB RAM (6 GB reservation)

c. Remote Expert Mobile—Large Machine

Requires 8 vCPU (16800 MHz reservation) and 8 GB RAM (8 GB reservation)

Select **Remote Expert Mobile— Singlebox (Developer)**, and click **Next**.

Step 10: Select the specific VMware host to run the template. Click **Next**.

Note: This host must have sufficient capacity to run the deployment VM configuration selected in the previous step.

a. If the host has been configured with multiple resource pools you may be required to select one.

b. If the host has multiple storages, you may be required to select one.

Step 11: Select the desired Disk Format and click **Next**.

The disk format chosen determines the way in which the virtual machine will allocate disk space, and when it will claim that space. The recommended format is **Thick Provision Lazy Zeroed**. Under this format, the entire disk space required by the guest OS (Remote Expert Mobile) will be allocated by the VMware host at template deployment time. However, disk blocks in the guest are zeroed at write time (making write operations slightly slower than the eager zeroed option).

Note: For developer lab deployments—you may choose Thin Provision. For most deployments, optimal performance is required—choose Thick Provision Eager Zeroed.

Step 12: Map the networks within the enterprise to those the template defines.

The OVA template will display the 3 interfaces (External, Internal and Management) that each require mapping to a network within the enterprise.

During deployment of the OVA, it automatically detects any available networks and randomly assigns one to the External, Internal and Management interfaces.

Note: These initial Interface-to-LAN mappings can be changed as required by double-clicking in the appropriate entry in the “Destination Networks” column.

As discussed earlier, for a single node deployment, the only interface required is the “External”. As the others will not be enabled, their associations are irrelevant.

Step 13: Check the box to power on the VM once deployment has completed, and click **Finish** to begin deployment.

Step 14: OVA installation will now proceed—wait for it to complete.

Step 15: Run the **setup.sh** script—see Running The Setup Script on page 28, then continue with the rest of the steps below

Step 16: Post install server access.

On first boot of the newly created VM, the OS and RE Mobile applications will be configured according to the details entered when executing the **setup.sh** script, so the first boot of the new VM will take longer than a normal boot.

Note: Please do NOT use the VM until the login prompt is displayed on the console, as viewed through the vSphere client.

To log into the external address of the VM, use SSH with the following credentials:
Username: `rem-ssh`
Password: `<user-configured>`

Then change to another user to perform any tasks—see REM Users and Security on page 11.

Note: To change the password after installation, see Changing Passwords on page 53.

Step 17: Perform Post Install Verification

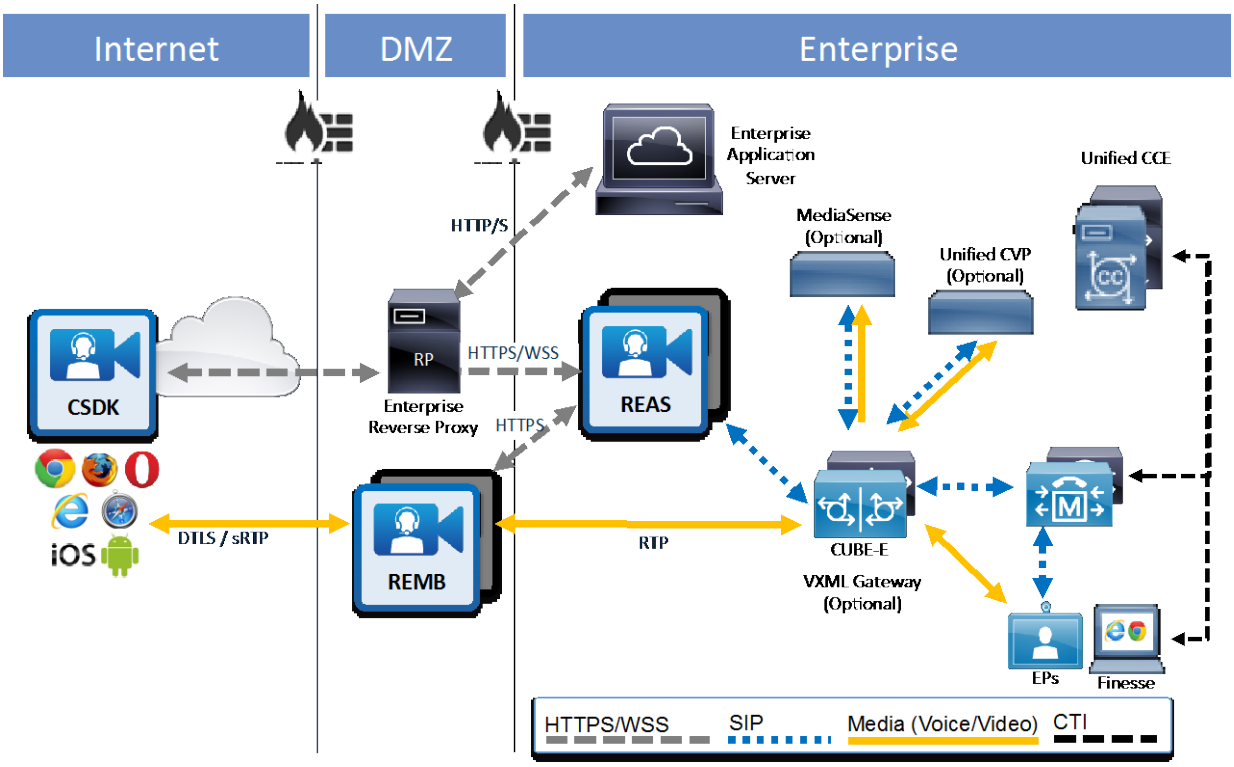
The single node deployment is now complete.

Verify that everything is in order by performing some post install tests outlined in Post-Install Verification on page 50.

Installing a Base Multi-node HA Deployment

Base Multi-node HA Topology Overview

Figure 3. Base Multi-node HA Deployment



Prior to installation of the **Base HA Multi-node** model, read the *Cisco Remote Expert Mobile—Design Guide* for better familiarity with Remote Expert Mobile pre-requisites, architecture and software components.

Note: The topology below is an example only.

Server Type	OVA Size	Type of Node	OVA Configuration Notes
REAS-A	Small	Master	Master: 0.0.0.0 (change from default to 0.0.0.0) External: 10.10.10.90
REAS-B	Small	Slave	Master: 10.10.10.90 External: 10.10.10.190
REMB-A	Large	Master	Master: 0.0.0.0 (default) External: 198.135.3.99 Internal(Optional): 10.10.10.95 Management (Optional): false
REMB-B	Large	Master	Master: 0.0.0.0 (default) External: 198.135.3.100 Internal(Optional): 10.10.10.195 Management (Optional): false

Installing and Configuring REAS (Base Multi-node HA deployment)

This section outlines how to deploy a Remote Expert Mobile Application Server (REAS) within a multi-node topology.

In production deployments, the REAS is installed and configured as separate VM from the REMB (Media Broker). The REAS cluster is installed and configured within the enterprise's internal "green" zone, while the REMB is within the DMZ.

A typical multi-node deployment consists of two REAS VMs and the REMB VMs for increased resilience and media-handling capabilities.

Required REAS and REMB Interfaces

The diagram below shows the recommended configuration of a multi-node topology in which the REAS VM(s) has been configured with its "External" interface on one network subnet, and an optional "Management" interface on a different network subnet.

> **Note**: the "Internal" interface has not been enabled on the REAS VM, as it is not used by this component.

As described earlier, enabling the "Management" interface on the REAS VM is an optional security measure, which forces its administration to be performed using a separate "Management" LAN subnet that is different to the one that the VM's "External" interface is connected to.

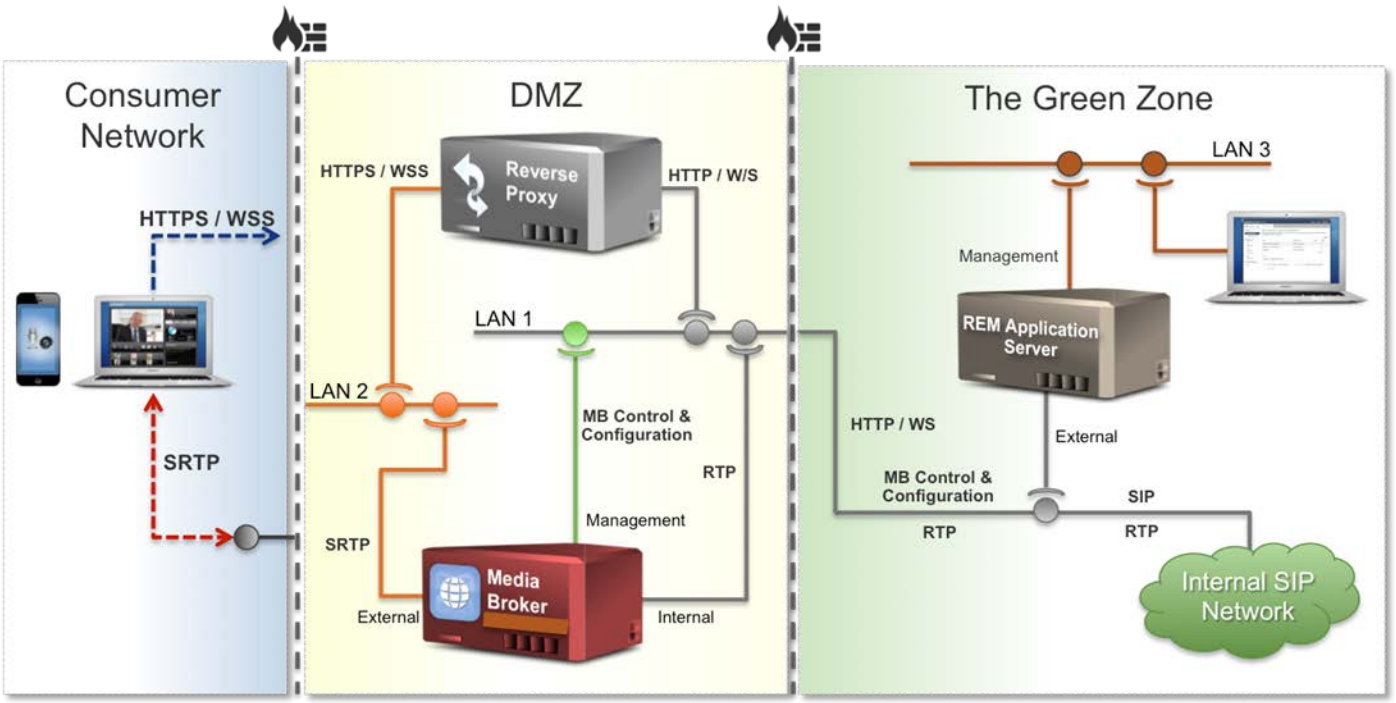
The diagram below also shows the recommended configuration of the REMB VM which has both "External" and "Internal" interfaces (connected to different network subnets within the DMZ) in order to segregate the media external and internal RTP traffic that it handles.

In addition to the "External" and "Internal" interfaces, the "Management" interface has also been enabled on the Media Broker VM. The Web Gateway uses this interface on the Media Broker to configure and control it.

Note: Remote Expert Co-browse should not have REMB nodes, and consequently does not needs interfaces configuring for them.

> **Note**: the diagram shows the LANs within the DMZ and in the Green Zone being terminated at the firewall; it is expected that the firewall between these distinct zones will act as a NAT router.

Figure 4. High Level Logical REAS Topology:



Installing the Remote Expert Mobile Application Server (REAS)

Note: for the base multi-node HA deployment, there are two REAS servers, one master and one slave; in a bigger multi-node HA deployment, there will be more than 2 REAS nodes defined. The following steps should be performed for each REAS.

Step 1: Download the RE Mobile OVA through your usual distribution channels.

Note: The OVA is a large file—allow sufficient time to download the OVA prior to beginning an installation.

Step 2: Launch the VMware vSphere client on your local machine and connect to your vCenter Server.

Step 3: Select the VMware Datacenter containing the VMware host you intend to deploy to.

Step 4: Click: **File** > **Deploy OVF Template…**

Step 5: Browse to locate the RE Mobile OVA file. Click **Next** .

Step 6: Review OVF image details and click **Next** to continue.

Step 7: Click **Accept** for each license agreement. When all license agreements have been accepted, click **Next.**

Step 8: Specify a name and location for the deployed template. Choose the VMware Datacenter containing the VMware host you intend to deploy into and click **Next**.

Note: The specific VMware host will be selected in a later step.
You may change the default template name to something more descriptive if you wish.

Step 9 (REAS): Select the desired hardware deployment configuration.

The deployment template enables you to choose from one of several VM *hardware* configurations. The supported configuration is the “small machine,” described below.

Remote Expert Mobile—Small Machine

Requires 4 vCPU (8400 MHz reservation) and 4 GB RAM (4 GB reservation)

Select a machine configuration supported by the capacity of your VMware Host, and click **Next**.

Step 10 (REAS): Select the specific VMware host to deploy the VM. Click **Next**.

Note: This host must have sufficient capacity to run the deployment VM configuration selected in the previous step.

- If the host has been configured with multiple resource pools, you may be required to select one.
- If the host has multiple storages, you may be required to select one.

Step 11 (REAS): Select the desired Disk Format, choose **Thick Provision Lazy Zeroed** and click **Next**.

The disk format chosen determines the way in which the virtual machine will allocate disk space, and when it will claim that space. The option selected will affect the deployment speed.

Thick Provision Lazy Zeroed

The entire disk space required by the guest OS (Remote Expert Mobile) will be allocated by the VMware host at template deployment time. However, disk blocks in the guest are zeroed at write time (making write operations slightly slower than the eager zeroed option).

Step 12 (REAS): Map the networks within the enterprise to those the template defines.

The OVA template will display the three interfaces (External, Internal and Management) that each require mapping to a network within the enterprise.

During deployment of the OVA, it automatically detects any available networks and randomly assigns one to the External, Internal and Management interfaces. These initial Interface-to-LAN mappings can be changed as required by double-clicking in the appropriate entry in the “Destination Networks” column.

The OVA deployment's next configuration screen will allow you to specify IP addresses for the various interfaces that are required.

As discussed earlier, for this Application Server VM being deployed, the only required interface is the "External" one. As the "Internal" interface does not apply to REAS, it will not be enabled (on the next screen), therefore its association is irrelevant.

Step 13 (REAS): Review the summary, check the box to power on the VM once deployment has completed, and click **Finish** to begin deployment.

Step 14 (REAS): OVA installation will now proceed—wait for it to complete.

Step 15 (REAS): Run the **setup.sh** script—see Running The Setup Script on page 28, then continue with the rest of the steps below.

Note: The first REAS needs to be set as Master; additional REAS and REMB nodes need to be set as Slave—select the node type at the **Enter Node type** prompt when you run the **setup.sh** script,

Step 16 (REAS): Post install server access.

On first boot of the newly created VM, the OS and RE Mobile applications will be configured according to the details entered when executing the **setup.sh** script, so the first boot of the new VM will take longer than a normal boot.

Note: Please do NOT use the VM until the login prompt is displayed on the console, as viewed through the vSphere client.

To log into the external address of the VM, use SSH with the following credentials:
Username: `rem-ssh`
Password: `<user-configured>`

Then change to another user to perform any tasks—see REM Users and Security on page 11.

Note: To change the password after installation, see Changing Passwords on page 53.

Step 16 (REAS): Adding an Additional REAS Slave Node

The instructions in this section can be repeated to install additional REAS VMs into the cluster.

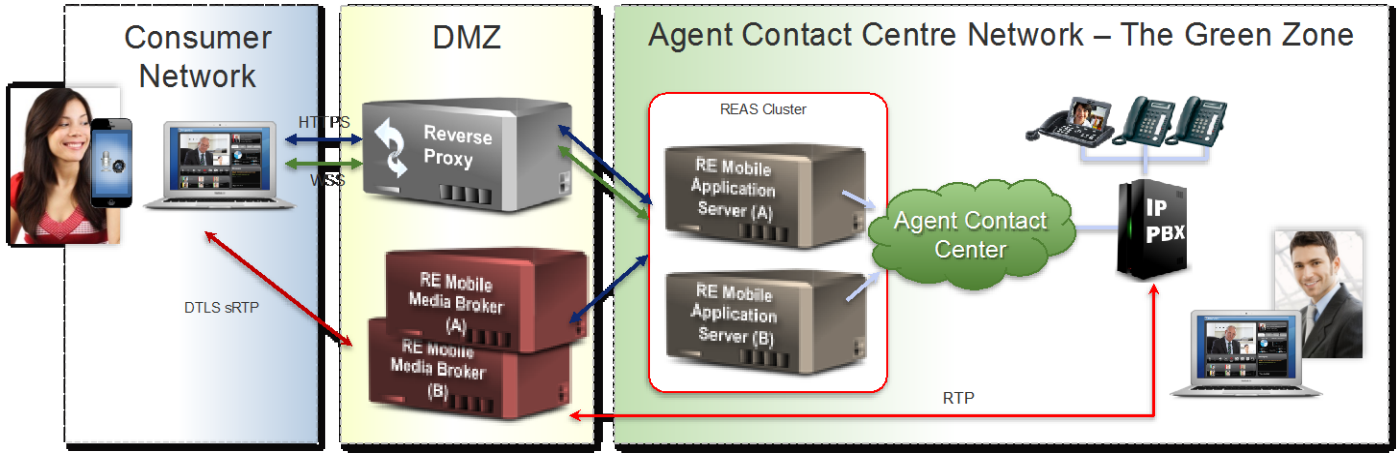
Installing and Configuring a REMB (Base Multi-node HA deployment)

Note: Skip this step for Remote Expert Co-browse.

The steps below outline how to install the REMB within a multi-node topology.

In a typical production deployment (see diagram below), each REMB would be installed onto a VM within the DMZ, which is separate to the REAS VM that is within the enterprise's internal "green" zone REMB should be installed after the REAS cluster has been established. Additional REMBs can be installed for more session capacity and as media handling needs increase.

Figure 5. Multi-Node Deployment



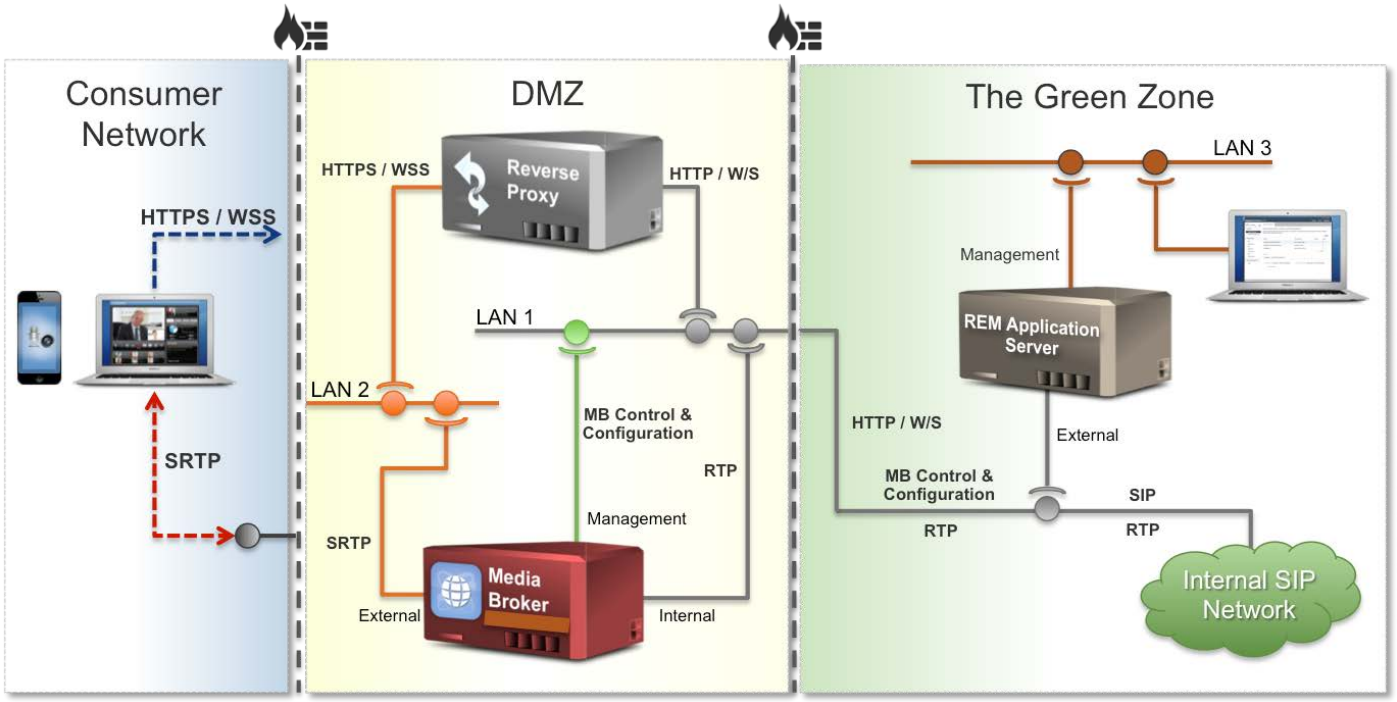
Required Interfaces

The diagram below shows the recommended configuration of a multi-box topology in which the Media Broker has been configured with both “External” and “Internal” interfaces (connected to different network subnets within the DMZ) to segregate the external and internal RTP traffic it handles.

In addition to the “External” and “Internal” interfaces, the “Management” interface has also been enabled on the Media Broker VM. The Web Gateway will use this interface to configure and control the Media Broker.

Note: The diagram below shows the LAN’s “Internal” interface of the Media Broker VM connected to LAN1. However, if required, this interface could be connected to a different LAN that is used to transport RTP between the DMZ and the internal SIP network within the DMZ and in the Green Zone being terminated at the firewall. It is expected that the firewall between these distinct zones will act as a NAT router.

Figure 6. Multi-Node Multi-NIC



OVA Deployment

The OVA will be deployed with a view to having the resulting VM just host the Media Broker in the DMZ.

Details of deploying a REAS are described in the **Installing an Application Server** section above.

To install the Remote Expert Mobile Media Broker, deploy the RE Mobile OVA template as described below.

Note: If REM Expert Assist is to be used *only* in co-browse-only mode, the Media Broker is not required.

Note: These instructions can be repeated to install additional Media Brokers.
All nodes in an REM cluster must be on the same subnet. If they are not, they cannot communicate without an appropriate routing infrastructure. The routing approach is strongly discouraged.

Step 1 (REMB): Use the previously downloaded RE Mobile OVA.

Step 2 (REMB): Launch the VMware vSphere client on your local machine and connect to your vCenter Server.

Step 3 (REMB): Select the VMware Datacenter containing the VMware host to which you intend to deploy.

Step 4 (REMB): Click File > Deploy OVF Template…

Step 5 (REMB): Browse to locate the RE Mobile OVA file (for example, `RE Mobile-11.5.1.10000-x.ova`)

Step 6 (REMB): Review OVF image details and click **Next** to continue.

Step 7 (REMB): Click **Accept** for each license agreement, then click **Next**

Step 8 (REMB): Specify a name and location for the deployed template. Choose the VMware Datacenter containing the VMware host that you intend to deploy into and click **Next.**

The specific VMware host will be selected in a later step.

Note: The default template name should be changed to something more descriptive, as this is helpful when performing a multi-node installation.

Step 9 (REMB): Select the **Large Machine** hardware deployment configuration.

Note: Base HA Multi-node deployments always require large OVA instances for all REMB instances.

Remote Expert Mobile—Large Machine

Requires 8vCPU (16800 MHz reservation) and 8 GB RAM (8 GB reservation)

Ensure that the Large Machine configuration is supported by the capacity of your VMware Host or physical server, and click **Next**.

Step 10 (REMB): Select the specific VMware host to run the template. Click **Next**.

Note: This host must have sufficient capacity to run the deployment VM configuration selected in the previous step**.**

a. If the host has been configured with multiple resource pools you may be required to select one.
b. If the host has multiple storages you may be required to select one.

Step 11 (REMB): Select the Disk Format **Thick Provision Lazy Zeroed** and click **Next**.

The disk format chosen determines the way in which the virtual machine will allocate disk space, and when it will claim that space. The preferred production format is:

Thick Provision Lazy Zeroed

The entire disk space required by the guest OS (Remote Expert Mobile) will be allocated by the VMware host at template deployment time. However, disk blocks in the guest are zeroed at write time (making write operations slightly slower than the eager zeroed option).

Step 12 (REMB): Map the networks within the enterprise to those the template defines.

The OVA template will display the 3 interfaces (External, Internal and Management) that each require mapping to a network within the enterprise.

During deployment of the OVA, it automatically detects any available networks and randomly assigns one to the External, Internal and Management interfaces. These initial Interface-to-LAN mappings can be changed as required by double-clicking in the appropriate entry in the "Destination Networks" column.

The OVA deployment's next configuration screen will allow you to specify IP addresses for the various interfaces that are required.

As discussed earlier, for this Media Broker VM being deployed, the required interfaces are the "External" and "Internal". As the "Management" interface will not be enabled (on the next screen), its association with a LAN is irrelevant.

Step 13 (REMB): Review the summary, check the box to power on the VM once deployment has completed, and click **Finish** to begin deployment.

Step 14 (REMB): OVA installation will now proceed—wait for it to complete.

Step 15 (REMB): Run the **setup.sh** script—see Running The Setup Script on page 28, then continue with the rest of the steps below.

Note: The first REAS needs to be set as Master; additional REAS and REMB nodes need to be set as Slave—select the node type at the **Enter Node type** prompt when you run the **setup.sh** script,

Step 16 (REMB): Post install server access.

On first boot of the newly created VM, the OS and RE Mobile applications will be configured according to the details entered when executing the **setup.sh** script, so the first boot of the new VM will take longer than a normal boot.

Note: Please do NOT use the VM until the login prompt is displayed on the console, as viewed through the vSphere client.

Once the VM has been installed, SSH into its external address and stop the REAS using the credentials below.

Username: `rem-ssh`

Password: <user-configured>

Then change to another user to perform any tasks—see REM Users and Security on page 11.

Step 17 (REMB): Configuring the Web Gateway Cluster with the REMB

Log into the RE Mobile Web Administration Console
`https://<Cluster IP or FQDN>:8443/web_plugin_framework/webcontroller/mediabrokers`
using the credentials you configured when you ran the **setup.sh** script.

a. Click the "**Add Record**" button to add a new record for the Media Broker that has just been installed.

b. Enter the "**Control Address**" (as shown below)—This should be the IP address of the REMB's control port. The control port will be bound to the management interface (if enabled) or the internal interface (if not enabled).

   The Web Gateway will use this address on the REMB to configure and control it.

c. Add a new "**SIP Network**" record.

d. **Local Address CIDR**—This is the address range the REMB will bind to for RTP communications on the SIP Network. Set this to the IP address of the "Internal" interface in CIDR format, that is **<IP-Address>/32**

e. **Start/Finish Port Ranges**—This is the port range the REMB will bind to on the SIP Network, for example, 17000 – 17500

   Each REMB will use 4 ports per call. As such, the number of ports required for the REMB to bind to on the SIP side is typically calculated as follows:

   Number of concurrent calls the REMB is expecting to manage X 4

f. Add a new "**WebRTC Client**" record—See the diagram above.

g. **Source CIDR Address**—This is the address range on which the REAS will receive WebRTC traffic from clients in CIDR format, for example, **all**

h. Click the '**+**' sign next to the newly added record and add entries defining the "**RTP Public and Local Port**"

i. **Public Address & Port**—This is the IP address and port that WebRTC clients must send RTP traffic to; typically, the front of a firewall, for example, 16000

j. **Local Address & Port**—This is the IP address and port the REMB will bind to in order to receive RTP traffic from WebRTC clients, for example, 16000

k. As the REMB now starts up with 5 processes it is now required that each Media Broker's Source CIDR Address is associated with 5 ports. To configure this, repeat steps **h.** to **j.** above to configure a total of 5 ports, for example, ranging from 16000 – 16004.

   Note: All of these ports will need to be opened on the firewall.

l. Click the "**Save**" button to persist the configured REMB.

   Note: It is possible to configure both internal (SIP) and external (WebRTC) interfaces to use the same IP address and ports. Typically, a SIP configuration will take a range of ports, while WebRTC configurations will take a single port. It is important that the WebRTC port be OUTSIDE of the SIP port range.

Step 18 (REMB): Configuring Additional Media Broker Nodes

The instructions in this section (Step 1 (REMB) to Step17 (REMB)) can be repeated to install additional Media Broker nodes into the cluster.

Step 19 (REMB): Post Install Verification

Your cluster deployment is now complete.

Verify that everything is in order by performing some post install tests outlined in the Post-Install Verification on page 50.

Running The Setup Script

Use the setup script to set up your installation of Remote Expert Mobile

Note: After installation, to change passwords, see Changing Passwords on page 53

After you have deployed your VM to the ESXi host, connect to the VM (for example, using vSphere) using the following credentials:

Username: `root`

Password: `changeit`

Run the script `setup.sh`

1. At the script prompts, enter the details as described in the following table, or press **Enter** to accept the existing setting.

Script Prompt	Setting (Default is shown in **bold**)	Notes
Enter REM OS User	**`rem-user`**	Enter a user name for the REM OS user— this is the user that uses REM, for example stops and starts the processes. Then follow the prompts to create the user and their password.
Enter REM OS Admin User	**`rem-admin`**	Enter a user name for the REM OS user— this is the user that administers REM, for example performs upgrades. Then follow the prompts to create the user and their password.
Enter SSH OS User	**`rem-ssh`**	Enter a user name for the SSH OS user—this is the user that is allowed SSH access to this machine. Then follow the prompts to create the user and their password.
Enter Server Type	`A` (REAS)	Install the first, or an additional, REAS **Note**: For Remote Expert Co-browse, only this value is applicable.
	`M` (REMB)	Install the first, or an additional, REMB
	`B` (Both)	Install an REAS and an REMB
Enter REAS Node type	**`M`** (Master)	The first REAS needs to be set as **Master**—additional REAS and REMB nodes need to be set as **Slave**.
	`S` (Slave)	
Enter Cluster Address	`reas.cisco.com`	This property is only required when installing a master REAS. Every Remote Expert Mobile Application Server cluster must consist of a single master node and from 1 – 9 slave nodes. The master node must be created prior to slave nodes being created. See Installing a Base Multi-node HA Deployment on page 20.
Enter Master Node Address		This property is only prompted for when installing REAS slave, or REMB node.

Script Prompt	Setting (Default is shown in **bold**)	Notes
Enter Hostname	`reas-a.cisco.com`	Specify the desired hostname of the VM being installed. This should be an FQDN.
Enter primary DNS Server		Enter the address of the primary DNS server that the RE Mobile VM will use.
Add/Edit another DNS Server?	**Y** N	Press **Y** to enter a secondary DNS server, or **N** to skip this.
Enter Secondary DNS Server		Enter the address of the secondary DNS server.
Use Network Time Server?	Y **N**	When installing a multi-node cluster, NTP must be configured by pressing **Y** and specifying an appropriate NTP server address.
Enter primary NTP Server	`time1.google.com`	Enter a primary network time server.
Add/Edit another NTP Server?	**Y** N	Press **Y** to enter a secondary NTP server, or **N** to skip this.
Enter secondary NTP server	`time2.google.com`	Enter a secondary network time server.
Enter system timezone	`UTC`	Set your timezone, for example `America/New_York`. For a full list of timezones in the correct format, see `https://en.wikipedia.org/wiki/List_of_tz_database_time_zones` or `http://www.iana.org/time-zones`
Enter External IP Address	`10.10.10.90`	Enter the IP address that will be assigned to this VM when installed. This must be a valid and available IP address within the network associated with the External interface.
Enter External Network Mask	`255.255.255.0`	Enter the required network mask for the network associated with the External interface.
Enter External Gateway	`10.10.10.1`	Enter the IP address of the External interface's network gateway.
Enter REMB Public Media Address	`10.10.10.90`	Set this to the publicly visible IP address for the REMB, if the External IP address is hidden behind Network Address Translation (NAT). If the Public Media IP Address is not set, it defaults to the External IP address, set above. Leave empty in Remote Expert Co-browse
	Y	

Script Prompt	Setting (Default is shown in **bold**)	Notes
Add/Edit Internal Network?	**N**	The Media Broker will be configured with 2 NICs—External and Internal. To enable and configure the Internal interface, press **Y**. In Remote Expert Co-browse, leave as default.
Enter Internal IP Address	`10.10.20.1`	Enter the IP address that will be assigned to this VM's Internal interface when installed. This must be a valid and available IP address within the network associated with the Internal interface.
Enter Internal Network Mask	`255.255.255.0`	Enter the required network mask for the network associated with the Internal interface.
Add/Edit Internal Network Static Route?	Y **N**	Configure the routing for this node to connect to the Internal network, if required. Entering values in these fields will add a static route to the VM's network routing table, enabling the Application Server to communicate with entities on a different network using this interface. Enter the IP address of the Internal interface's gateway, and enter the network address in CIDR format, for example 10.10.10.0/24. Using an Internal network is not mandatory, so these fields can be left blank if required.
Enter Internal Gateway?	`10.10.20.1`	
Enter Internal Gateway Remote Network (CIDR Format)	`10.10.10.0/24`	
Add/Edit Management Network?	Y **N**	The management interface can be enabled for REMB, if it is enabled then the REMB control port (8092) used by REAS will be bound to the management IP address. Leave as default for Remote Expert Co-browse.
Enter Management IP Address	`10.10.30.90`	
Enter Management Network Mask	`255.255.255.0`	
Add/Edit Management Network Static Route?	Y **N**	Configure the routing for this node to connect to the Management network, if required. Entering values in these fields will add a static route to the VM's network routing table, enabling the Application Server to communicate with entities on a different network using this interface. Enter the IP address of the Internal interface's gateway, and enter the network address in CIDR format, for example 10.10.10.0/24. Using a Management network is not mandatory, so these fields can be left blank if required.
Enter Management Gateway	`10.10.30.1`	
Enter Management Gateway Remote Network (CIDR Format)	`10.10.10.0/24`	

2. If the appliance has not yet been configured, the following prompts are displayed, then the script finishes and completes the setup:

Script Prompt	**Setting** (Default is shown in **bold**)	Notes
Enter new root password		Set the new OS root password
Retype new root password		
Enter new Expert Assist Admin username	`admin`	The Expert Assist Admin credentials are used for authenticating user access to both the REM Web Admin Console and the REAS Management Console.
Enter new Expert Assist Admin password		
Retype new Expert Assist Admin password		
Enter new Remote Expert AS master/slave username	`master`	The Remote Expert AS master/slave credentials are used for authenticating access to the master node from any slave nodes (that is, this is not for user access). The same master/slave credentials need to be used across all REAS nodes in the cluster. **Note:** The username and password cannot be identical to each other.
Enter new Remote Expert AS master/slave password		
Retype new Remote Expert AS master/slave password		
Continue with setup?	**Y**	The script finishes and completes the setup—to continue with the post-install steps, as required, return to one of the following: • Step 16 on page 19; • Step 16 (REAS) on page 23; or • Step 16 (REMB) on page 26.
	`N`	The script exits without saving any settings. **Note:** Selecting this option cancels any entries that you have made—you will need to re-run the script and re-enter any settings, as required.

3. Alternatively, if the appliance has already been configured, or if the setup script is run for a second or subsequent time, the following prompts are displayed:

Script Prompt	**Setting** (Default is shown in **bold**)	Notes
Accept the agreement Y/N?	Y N	Accept the agreement
Certificate was added to keystore		
Please enter the Expert Assist Admin username	admin	The Expert Assist Admin credentials are used for authenticating user access to both the REM Web Admin Console and the REAS Management Console. These must match the Expert Assist Admin credentials used in the system you are upgrading from.
Please enter the Expert Assist Admin password		
Please enter the REAS master/slave username	master	The new Remote Expert AS master/slave credentials are used for authenticating access to the master node from any slave nodes (that is, this not for user access). These need not match any credentials used in the system that you are upgrading from. The same master/slave credentials need to be used across all REAS nodes in the cluster. **Note:** The username and password cannot be identical to each other.
Please enter the REAS master/slave password		
Enter a root password for the new system. New password		Select this option to reset your existing REAS username and password. The system will prompt you to enter and confirm the new username and password
Retype new password		
Continue with setup?	**Y**	The script finishes and completes the setup—to continue with the post-install steps, as required, return to one of the following: • Step 16 on page 19; • Step 16 (REAS) on page 23; or • Step 16 (REMB) on page 26.
	N	The script exits without saving any settings. **Note:** Selecting this option cancels any entries that you have made—you will need to re-run the script and re-enter any settings, as required.

Connection Monitoring

As explained above, a Media Broker will typically be configured with multiple network interfaces. If there is more than one network interface and the management REST interface is bound to a different network than one or more of the media-carrying interfaces (internal or external) then it is possible for the Media Broker to process calls (via the REST interface) but be unable to send or receive media for those calls. To ensure that the Media Broker only accepts calls over the REST interface when it is fully connected to the internal and/or external networks you can configure connection monitoring.

Note: Remote Expert Co-browse has no Media Brokers, so this section does not apply.

How it works

Each Media Broker can be configured with none or more groups of addresses. A Media Broker will consider itself connected, and therefore able to service calls, if it can “reach” at least one of the addresses in each group. i.e. the logical operations are ORs within each group and ANDs between each group. The Media Broker will attempt to establish the “reachability” of an address by:

- ping (ICMP echo requests)
- If that receives no response then attempt to establish a TCP connection to port 7 at that address

A success with either mechanism will mark that address as reachable.

If there are no groups configured, then the Media Broker is considered to be connected.

Example

A typical network setup for Media Broker has three network interfaces:

- Management—The REST interface used by the Gateway is bound to this addresses
- External—external media
- Internal—internal media

In this case there is no need to monitor connectivity on the management interface, as the gateway will only use the Media Broker if it can reach it over this interface. Therefore, it is sensible to monitor the external and internal interfaces.

Configuration and use of Transport Layer Security (TLS) in REAS

Overview of TLS and certificates

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. The owner encrypts the sent data using the recipient's public key, which can then be decrypted only with the private key in the pair. Encryption alone provides no proof of the identity of the sender of the encrypted information, however. Certificates address this problem by also providing a digital signature, an electronic means of verifying a resource's identity. To prove its identity, a resource requests a certificate from a Certification Authority (CA). The issued certificate is then signed with the CA's private key, and should be added to the resource's identity certificate store. A certificate typically contains the following information:

- Owner's public key
- Owner's name
- Expiration date of the public key
- Name of the issuer (the CA that issued the certificate)
- Serial number of the certificate
- Digital signature of the issuer

This certificate can then be sent to other resources to establish trust with that resource. The receiving resource should add the CA certificate to their trust certificate store. For two-way trusted communication, certificates should be exchanged between resources.

All REAS components within a cluster should be provisioned with certificates signed by a trusted CA. During the installation process, the installer provisions the servers with temporary certificates, the CN (Common Name) of which reflects the cluster address that you specified when installing each component; this defaults to the external address of the server. The temporary certificates all have a common signer and as such it is possible for each of the servers within the cluster to communicate over TLS with other servers within the cluster. When the installation of the cluster has been completed, the certificates should be replaced with certificates that have been signed by a third-party Certification Authority (CA) or by a SCEP server. The CN in the updated certificates should reflect the fully-qualified DNS names of the Server Group. If all of the cluster components share the same CN, only one signed certificate will be required for the cluster.

Certificates can be managed using the REAS Management Console, and you can manage the certificates for multiple Server Groups. The REAS Management Console enables you to perform the following functions:

- view identity certificates
- create and sign new identity certificates using SCEP
- create Certificate Signing Requests (CSRs) for third-party CAs
- replace existing identity certificates, for example, when they are about to expire, or the CN value has changed (host or domain renamed)
- replace expired identity certificates
- view trust certificates
- import trust certificates.

To work with certificates, you must know the security password; the default password is `changeit`, however this might have been changed after installation.

Note: Certificates are initially created on the VM instance hosting the Master REAS, and are then automatically copied to all of the REAS in the cluster.

Identity and trust certificate groups

An identity certificate is a certificate that can be used to identify a machine. The CN of these certificates will usually contain either:

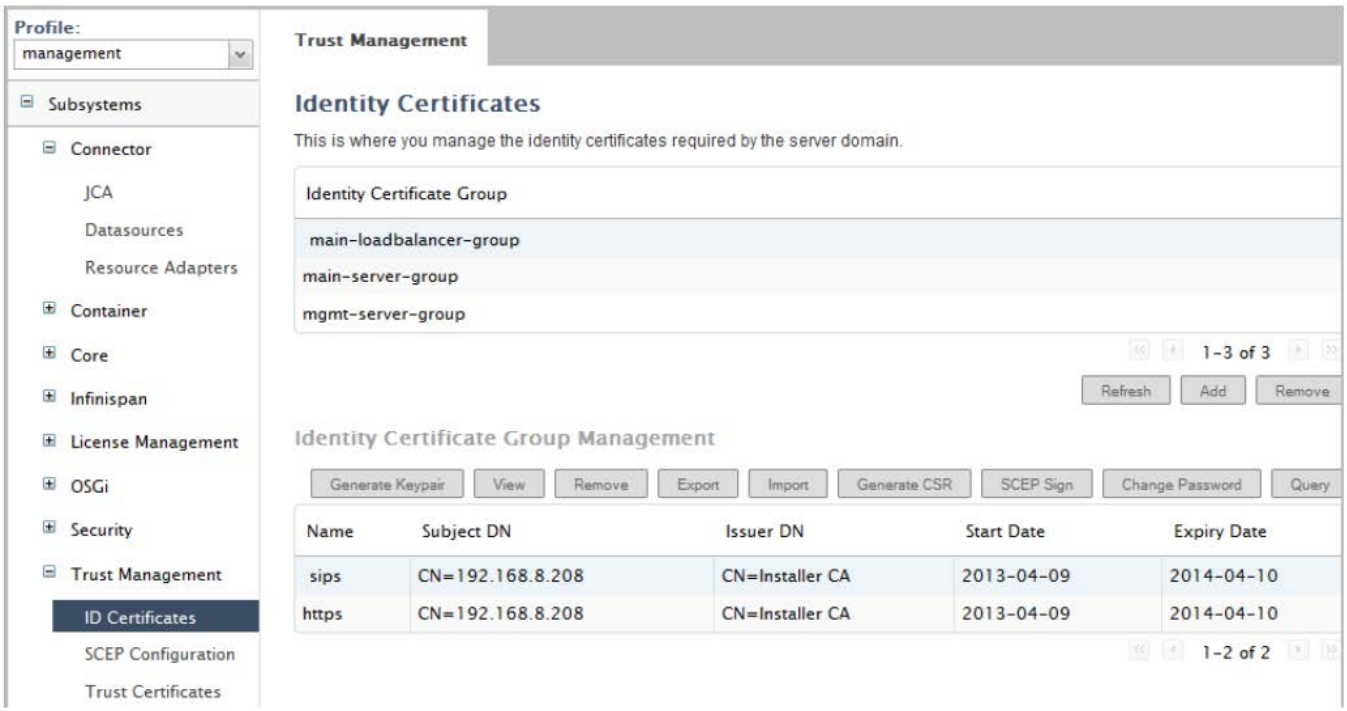
- A fully-qualified name that can be resolved in DNS. This name can resolve to one or more machines.
- The IP address of the machine.

To manage the certificates, log in to the following URL, using the credentials that you provided when executing the setup script: `https://<Cluster IP or FQDN>:9990` **> Trust Management**

Identity certificates are managed in 'identity certificate groups'. On installation, the following identity certificate groups are created:

- mgmt-server-group - for the Master REAS (Domain Host Controller), that is, the server hosting the REAS Management Console and the License Server.
- main-server-group for the REAS.

For example:



For the REAS groups, a certificate is required for each transport type (SIPS and HTTPS) in the group, as shown in the image above. As the Master REAS (Domain Host Controller) is only a management interface, only an HTTPS certificate is required.

Trust certificates are managed in 'trust certificate groups'. By default, a single trust certificate group is created, which can be used by all of your Server Groups.

Certificates are created and saved in identity certificate group and trust certificate group directories on the server hosting the Master REAS (Domain Host Controller), and are then automatically copied to each REAS in the Server Group.

If a new REAS is added to an existing Server Group, the certificate group directories are automatically copied to that new server. Similarly, if a new cluster, or Server Group, is added to the enterprise, the certificate group directories are automatically copied to each REAS in the new cluster.

Configuring REAS with identity certificates signed by a third-party CA

If you want to generate a new identity certificate to be signed by a third-party CA, you must generate a Certificate Signing Request (CSR), send the generated CSR to the third-party CA, and then import the signed certificate (received from the CA) into the identity certificate group.

Note: Certificates can also be signed by a SCEP server. See "Configuring Load Balancers or Application Servers with identity certificates signed by a SCEP server"**.**

If you want to generate a new certificate with a new name, you must first generate a key pair for the new certificate, and then follow the signing procedure using the newly generated entry in the list.

Generating a keypair

This step is only required if you are creating a certificate with a new name. If you just want to change the CN in the certificate, you do not need to generate a new keypair.

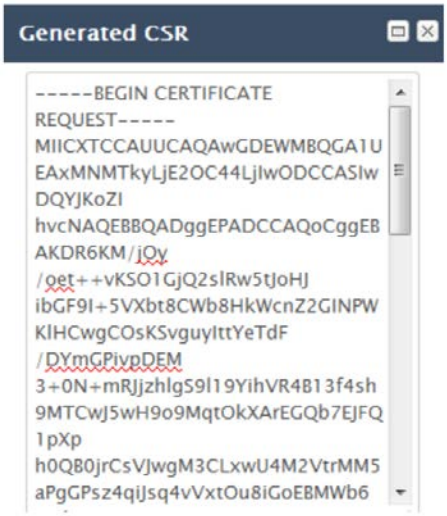
1. Log into the REAS Management Console `https://<Cluster IP or FQDN>:9990`, and from the top-right menu select Profiles.
2. From the Profile drop-down list, select the management profile.
3. From the menu on the left, expand Subsystems > Trust Management and select ID Certificates.
4. Select the identity certificate group that you want to work with.
5. Click Generate Keypair.
6. Enter a meaningful name, preferably indicating the component and transport type, for example, for a certificate for SIP traffic on Load Balancers, it could be called something like sip-lb.
7. Enter the DN value. The CN value in the DN should reflect that of the SIP domain. If the Load Balancers are in a different domain to the Application Servers, use the domain applicable to the component type that the new certificate is for). For example: `CN=192.168.1.234`, or `CN=example.net`.
8. Enter the expiry date, in the form `yyyy-mm-dd`. For example: `2015-03-20`.
9. Enter the security password.
10. Click **Save**.
    A new entry with the specified name is added to the list of certificates.

Generating a CSR

You need to generate a Certificate Signing Request to send to the third-party CA.

1. Log into the REAS Management Console `https://<Cluster IP or FQDN>:9990`, and from the top-right menu select **Profiles**.
2. From the Profile drop-down list, select the management profile.
3. From the menu on the left, expand **Subsystems > Trust Management** and select **ID Certificates**.
4. Select the identity certificate group that you want to work with.
5. Select the certificate that you want to be signed in the list; this might be the entry for the keypair that you have just generated.
6. Click Generate CSR.

7. Enter the security password, and the DN for the component that you are generating a certificate for, then click **Save**. A dialog containing the CSR text is displayed. For example:



8. Copy all of the displayed text, including the start and end tags, and paste it into a text editor, then save the file.
9. Click **Close**

Sending a certificate to the external CA for signing

The procedure for getting your certificate signed by a third-party CA depends upon the requirements of that CA. See the guidance from the CA.

Importing the signed certificate

When you receive the certificate back from the CA you must then import it into the identity certificate group.

1. In the **Identity Certificates** dialog, select the identity certificate group that you want to work with.
2. Select the certificate entry of the identity certificate that you requested the CSR for. You must ensure that you select the correct entry.
3. Click **Import**.
4. Enter the name of the certificate and the security password.
5. Open the certificate in a text editor, and copy all of the contents, including the start and end tags.
6. In the Encoded Certificate field, paste the certificate text.
7. Click **Save**.
8. Once the certificate is imported, the window is updated to reflect any changed certificate details, such as the issuer DN and the expiry date.
9. The updated identity certificate group directory is then copied to each Application Server and Load Balancer in the Server Group. Each server must be restarted for the changes to take effect.

Configuring Load Balancers or Application Servers with identity certificates signed by a SCEP server

If you want to generate a new certificate that is signed using the SCEP protocol, this is a single UI operation, which performs the CSR generation, sending, receiving, and importing steps automatically. Before you can perform this procedure, you must configure the REAS with the details of a server that implements the SCEP protocol, for example, an EJBCA server.

Configuring REAS to use the SCEP protocol

1. Log into the REAS Management Console `https://<Cluster IP or FQDN>:9990`, and from the top-right menu select **Profiles**.
2. From the **Profile** drop-down list, select the management profile.
3. From the menu on the left, expand **Subsystems** > **Trust Management** and select **SCEP Configuration**.
4. Click **Add**.
5. Enter the required SCEP values as follows:

Parameter	Value
Name	Enter a name for this SCEP configuration
URL	The SCEP Server CGI URL. A typical value for an EJBCA server might be something like: http:// ejbca.example.com:8080/scepraserver/scep/ pkiclient.exe
Profile	Enter the value of the SCEP profile, or identity, that you want to use
Subject DN Prefix	This is the string that will be prefixed to the “CN=” value when constructing the Subject Distinguished Name in the X509 certificate. For example, if this field is set to “C=GB,O=Cisco,OU=Test”, the subject DN might be something like “C=GB,O=Cisco,OU=Test,CN=example.com”.

6. Click **Save**.

Generating a SCEP-signed certificate

1. In the **Identity Certificates** dialog, select the identity certificate group that you want to work with.
2. If you want to create a certificate with a new name, you first need to generate a keypair. See Generating a keypair on page 36.
3. Select the certificate entry of the identity certificate that you want to send to the SCEP server for signing.
4. Click **SCEP Sign Certificate**.
5. The CSR is generated, sent to the SCEP server, signed, returned, and imported into the identity certificate group directory.
6. The updated identity certificate group directory is then copied automatically to each Application Server and Load Balancer in the Server Group.
7. Each server hosting an REAS must then be restarted for the changes to take effect.

Configuring REAS with trust certificates

To allow TLS connections from the REAS to external entities that use self-signed certificates or identity certificates signed by a CA that is not currently recognized, the self-signed or CA certificate must be added to the trust certificate group.

Importing the trust certificate

1. Log into the REAS Management Console `https://<Cluster IP or FQDN>:9990`, and from the top-right menu select **Profiles**.
2. From the **Profile** drop-down list, select the **management** profile.
3. From the menu on the left, expand **Subsystems** > **Trust Management** and select **Trust Certificates**.
4. Select the trust certificate group that you want to work with.
5. Click **Import**.
6. Enter a meaningful name, preferably indicating the CA/identity whose certificate you want to import, and the security password.
7. Open the certificate from the unknown CA/identity in a text editor and copy all of the contents, including the start and end tags.
8. In the Encoded certificate field, paste the certificate text, and click **Save**.
   The certificate is imported into the trust certificate group directory and then copied to each server in the group.

Configuring the Domain Host Controller and License Server with an identity certificate

The Master REAS also has an identity certificate used for management purposes (for example, the REAS Management Console). On installation, this server is provisioned with a default, self-signed, identity certificate, in the management-group identity certificate group. This certificate should also be replaced with an alternative certificate signed by a third-party Certification Authority (CA) or a SCEP server.

1. Log into the REAS Management Console `https://<Cluster IP or FQDN>:9990`, and from the top-right menu select **Profiles**.
2. From the menu on the left, expand **Subsystems** > **Trust Management** and select **ID Certificates**.
3. In the **Identity Certificate Group** area, select **management-group**.
4. Do one of the following:
   a. If you want the certificate to be signed by the SCEP server, click **SCEP Sign Certificate**.
   b. If you want the certificate to be signed by a third-party CA, generate a CSR (see Generating a CSR on page 36), send it to the CA and then import the new certificate. (As this certificate is created and imported on the server that is hosting the Domain Host Controller that you are provisioning, no file transfer is required.)
5. Restart the server that is hosting the Domain Host Controller

Replacing an identity certificate

You would typically need to replace an identity certificate when it has expired.

1. Log into the REAS Management Console `https://<Cluster IP or FQDN>:9990`, and from the top-right menu select **Profiles**.
2. From the **Profile** drop-down list, select the **management** profile.
3. From the menu on the left, expand **Subsystems** > **Trust Management** and select **ID Certificates**.
4. Select the identity certificate group that you want to work with.
5. Select the certificate entry of the identity certificate that you want to replace.
6. Do one of the following:
    a. If you want the certificate to be signed by the SCEP server, click **SCEP Sign Certificate**.
    b. If you want the certificate to be signed by a third-party CA, generate a CSR (see Generating a CSR on page 36), send it to the CA and then import the new certificate.
7. The updated identity certificate group directory is then copied automatically to each Application Server and Load Balancer in the Server Group.
8. Each server hosting an Application Server or Load Balancer must then be restarted for the changes to take effect

Exporting an identity certificate

If you want to create a backup copy of a certificate signed by a third-party CA, you can do so by exporting it.

1. Log into the REAS Management Console `https://<Cluster IP or FQDN>:9990`, and from the top-right menu select **Profiles**.
2. From the **Profile** drop-down list, select the **management** profile.
3. From the menu on the left, expand **Subsystems** > **Trust Management** and select **ID Certificates**.
4. Select the identity certificate group that you want to work with.
5. Select the certificate entry of the identity certificate that you want to export.
6. Click **Export**.
7. Enter the KeyStore password—the default password is `changeit`
   A dialog containing the certificate text is displayed.

   See also: Changing the KeyStore Password on page 54.
8. Copy the text and paste it into a text editor, then save the file.
9. Click **Cancel** to close the dialog.

Removing a trust certificate

You would typically remove a trust certificate to prevent TLS connections to machines that use either identity certificates signed by a specific CA, or self-signed identify certificates that you no longer trust.

1. Log into the REAS Management Console `https://<Cluster IP or FQDN>:9990`, and from the top-right menu select **Profiles**.
2. From the **Profile** drop-down list, select the management profile.
3. From the menu on the left, expand **Subsystems** > **Trust Management** and select **Trust Certificates**.
4. Select the trust certificate group that you want to work with.
5. Select the trust certificate that you want to remove.
6. Click **Remove**.
7. Enter the security password and click **Save**.
8. The updated identity certificate group directory is then copied automatically to each Application Server and Load Balancer in the Server Group.
9. Each server hosting an Application Server or Load Balancer must then be restarted for the changes to take effect.

Operating System

When the OVA has been successfully installed, and you have run the **setup.sh** script, you can SSH into the operating system using the following credentials:

Username: `rem-ssh`

Password: <rem-ssh password>

You can then change to another user to perform whatever tasks you need—see REM Users and Security on page 11.

To change these credentials after installation— see Changing Passwords on page 53.

Remote Expert Mobile Web Administration Console

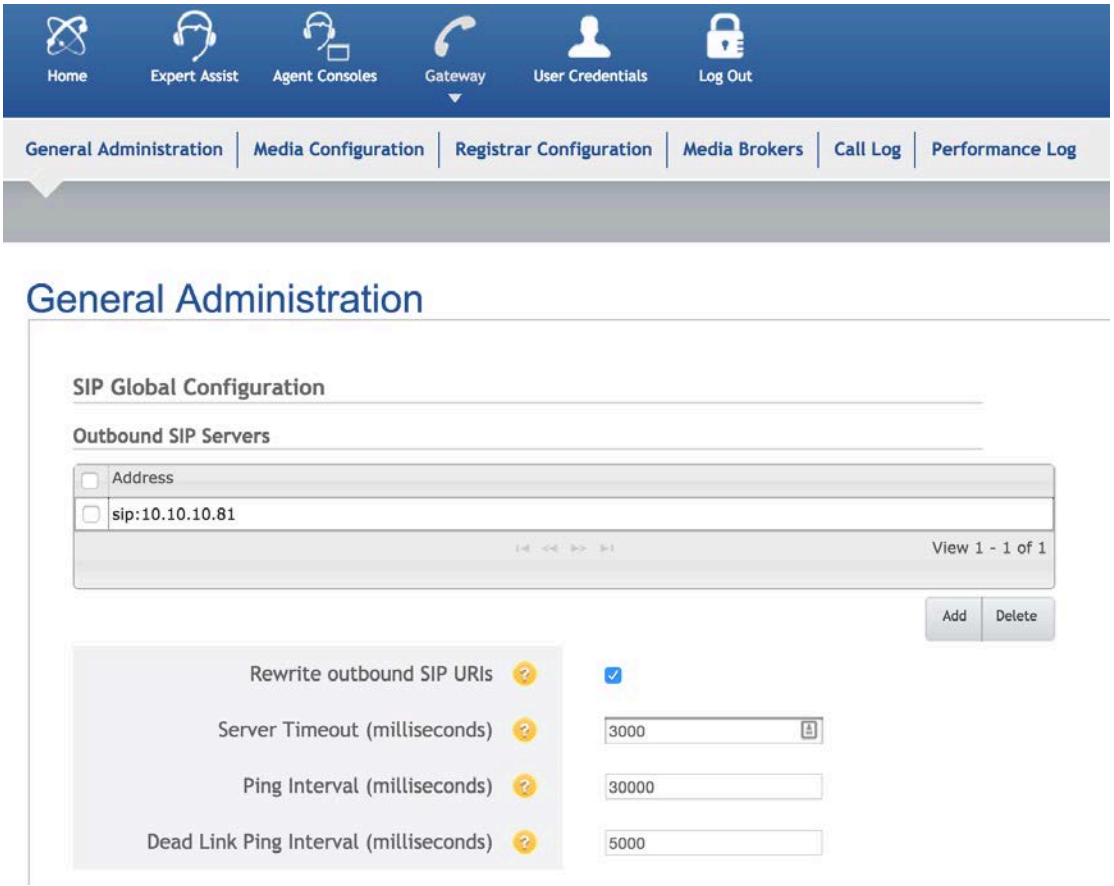
Log into the RE Mobile Web Administration Console
`https://<Cluster IP or FQDN>:8443/web_plugin_framework/webcontroller`
using the credentials you configured when you ran the **setup.sh** script.

RE Mobile Gateway Configuration—Outbound SIP Server

Note: In Remote Expert Co-browse, SIP is not flowing through the REM Gateway, so outbound SIP servers are not needed.

As SIP messages will need to be routed from REAS to the CUBE or direct to CUCM, the addresses of all the nodes within the CUBE cluster, or CUCM cluster if going direct, must be configured as an Outbound Sip Servers via the **Gateway** > **General Administration** page.

The format of the Outbound Sip Server URI is: **sip:<CUBE-OR-CUCM-IP-ADDRESS>** (, for example, sip:10.10.10.81 as shown below)



The meaning of these fields is as follows:

- **Rewrite outbound SIP URIs—**If this is set to *true* then REAS will update the host part of the Request URI of all outbound requests to match the host part of the outbound SIP server address. If this is set to *false* then requests are sent on to the outbound SIP server(s) without change.
- **Server Timeout—**The time REAS will allow a server to respond to a request before it is considered to be down before trying another server.
- **Ping Interval—**The interval between successive OPTIONS messages being sent to an outbound SIP server when that server is considered UP.
- **Dead Link Ping Interval—**The interval between successive OPTIONS messages being sent to an outbound SIP server when that server is considered DOWN.

REAS will maintain a view of whether it is connected to each of the outbound servers by examining the responses to OPTIONS messages and the responses to initial requests. The state of the Outbound SIP Server connections can be viewed in the performance log screen which can be found at **Gateway** > **Performance Log**.

When routing a new initial outbound request, the REAS will build up an ordered list of Outbound SIP Servers as follows:

1. First, all UP servers are added in a random order.
2. The remaining (DOWN) servers are appended to the list

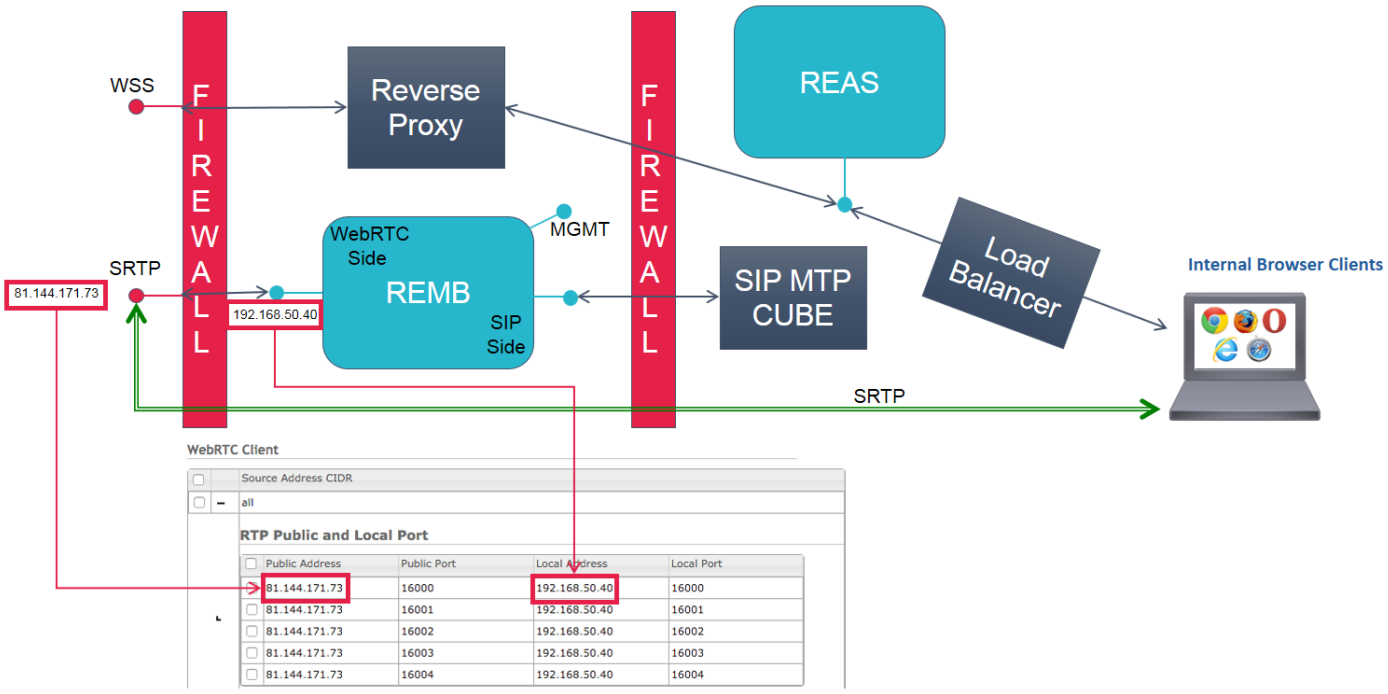
REAS will then route the request to the first in the list. If no response is received within the configured 'Server Timeout' period, then the request will be routed to the next server in the list and so on until a response is received or no more servers remain. In this latter case the call will fail.

REMB Settings in UCCE, UCCX, and UC Environments

Note: In Remote Expert Co-browse, there is no REMB. Consequently, WSS traffic is the same in each scenario.

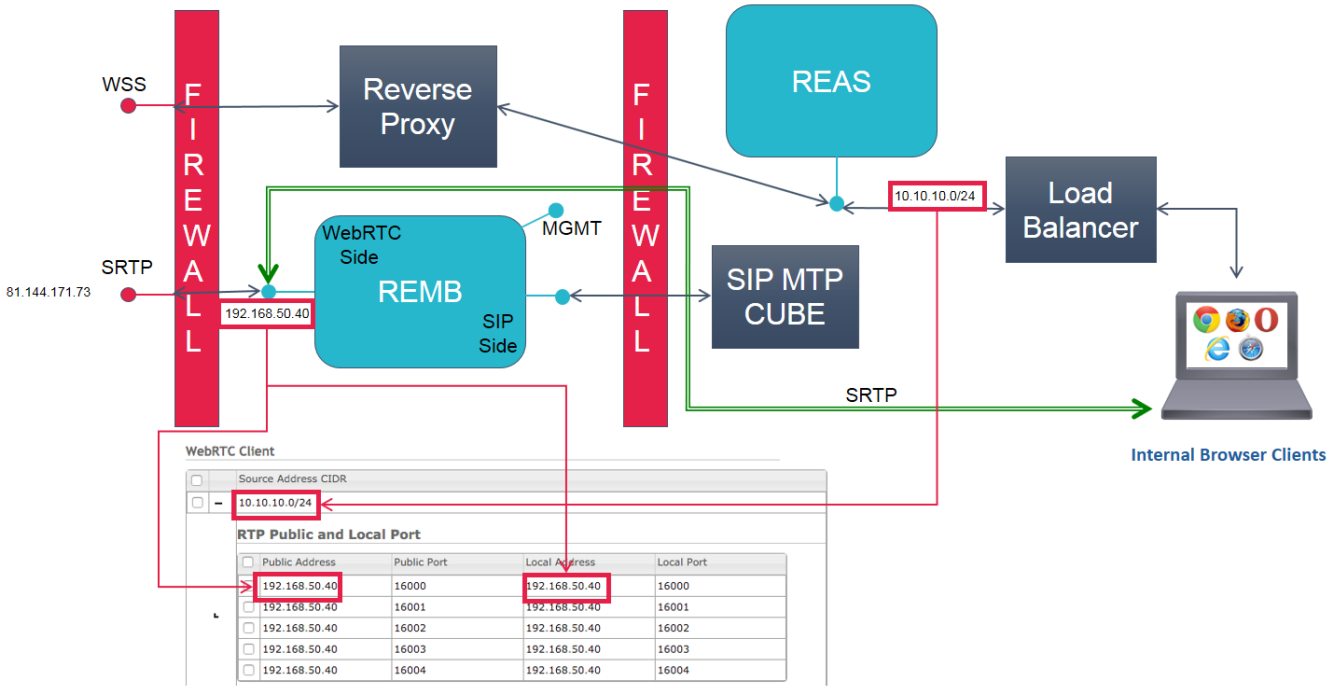
Configuring the RTP public and local port settings correctly enables agents to operate whether they are internal or external to the network. See the following topology diagrams for details of how to configure these settings in several different scenarios.

Scenario 1—REMB Public IP Address is Routable/Reachable



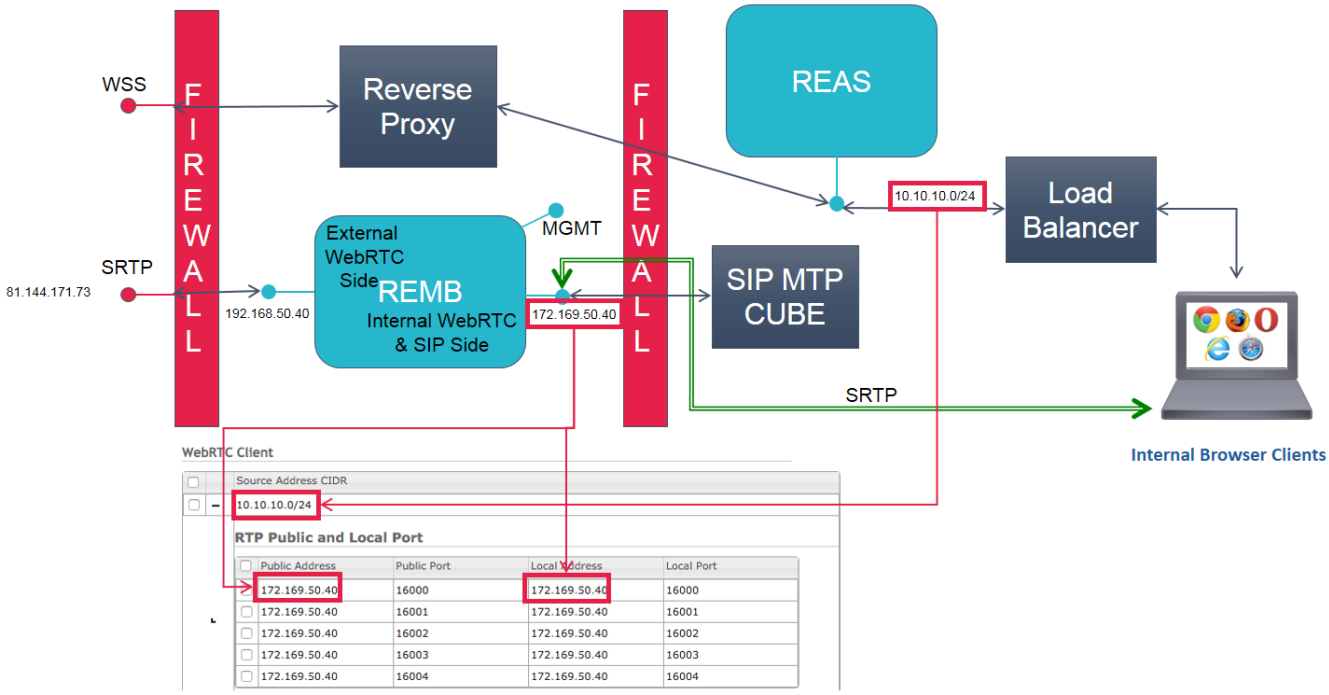
In this scenario, an agent on the internal network or on an external network (a source address of 'all' networks) can make a connection using the external/public IP address (for example, 81.144.171.73); this is matched to the WebRTC external-facing side of the REMB (for example, 192.168.50.40)—see the green connector in the diagram.

Scenario 2—REMB WebRTC-side Local IP Address is Routable/Reachable



In this scenario, an agent on the internal network (a source address of for example, 10.10.10.0/24) can make a connection using the WebRTC-side IP address (for example, 192.168.50.40); this same external-facing address is referred to as the 'public' and the 'local' address of the REMB—see the green connector in the diagram.

Scenario 3—REMB SIP-Side Local IP is Routable/Reachable



In this scenario, an agent on the internal network (a source address of for example, 10.10.10.0/24) can make a connection using the WebRTC internal-side IP address (for example, 1172.169.50.40); this same internal-facing address is referred to as the 'public' and the 'local' address of the REMB—see the green connector in the diagram.

Expert Assist Configuration—Consumer Access Number Regex

Note: In Remote Expert Co-browse, the consumer cannot dial a number through the REAS, and can be ignored or set to an invalid value.

Remote Expert Assist can be configured to limit the URIs that the consumer can dial.

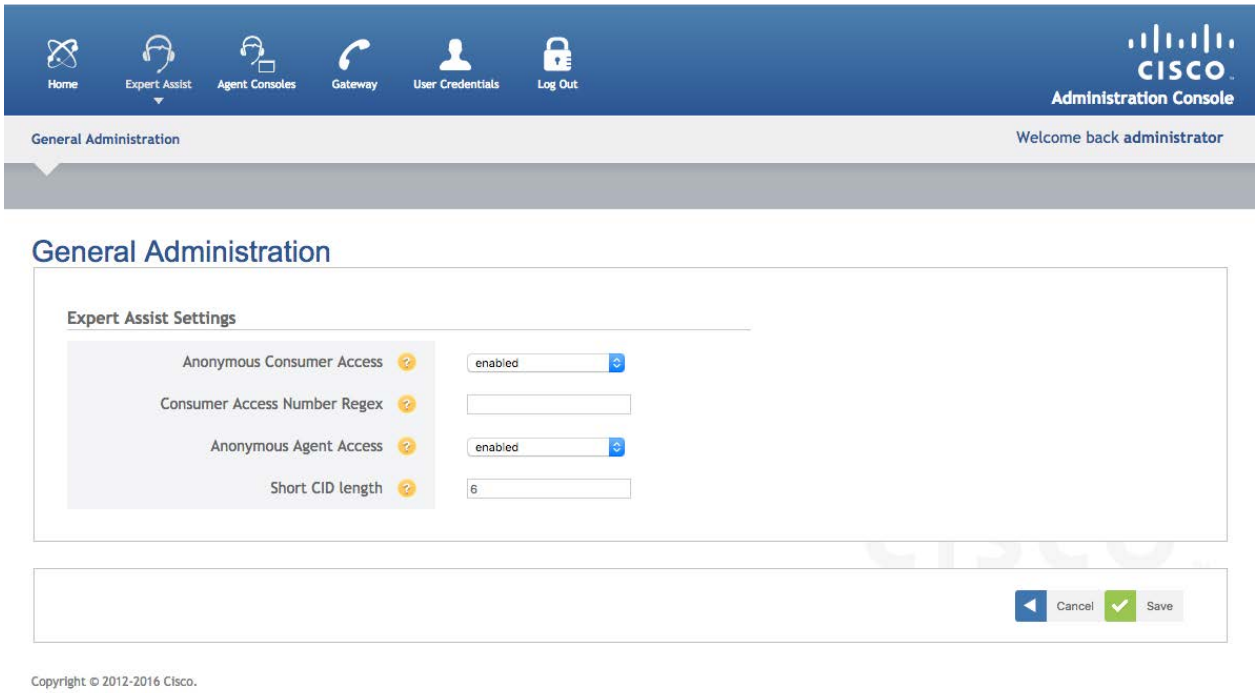
The consumer JavaScript API can specify the destination URI that it wishes to connect to. This is specified as a SIP URI and is typically set to an address on the CVP server (for example, sip:60017@100.1.0.100).

To avoid malicious users from changing this value it is possible to configure the Remote Expert Assist cluster with a regular expression that the destination provided by the consumer's browser must match. This configuration item is called the **Consumer Access Number Regex** and by default is blank, meaning it will allow calling to any destination.

The following steps outline how to lock down the range of addresses that the consumer may dial.

1. Log into the RE Mobile Web Administration Console
   `https://<Cluster IP or FQDN>:8443/web_plugin_framework/webcontroller`
   using the credentials you configured when you ran the **setup.sh** script.

2. Navigate to the **Expert Assist** tab and click the **General Administration** menu.



3. Edit the **Consumer Access Number Regex** field with a regular expression suitable for your deployment environment, for example, To only allow calls to the destination: sip:60017@100.1.0.100, enter the regex: `^sip:60017@100.1.0.100$`

4. Click **Save**.

To test that the Agent Console is working as required, follow the steps outlined in the **Testing the Agent Console** section of the **Post Install Verification** chapter.

Expert Assist Configuration—Enabling UUI Data

Note: In Remote Expert Co-browse, UUI data cannot be used, and this section should be ignored

Remote Expert Assist can be configured to allow User-to-User Information (UUI) to be passed from the client.

The value specified will be placed in the SIP User-to-User Information header in hex-encoded form.

Note: The UUI can only be used when “Anonymous Consumer Access” is set to “trusted” mode.

The "Anonymous Consumer Access" is a configuration item of RE Mobile and can be changed via the Expert Assist Administration page on the Web Plug-in Framework web console.

1. Log into the RE Mobile Web Administration Console
   `https://<Cluster IP or FQDN>:8443/web_plugin_framework/webcontroller`
   using the credentials you configured when you ran the **setup.sh** script..

2. Navigate to the **Expert Assist** tab and click the **General Administration** menu.

3. The property is called " Anonymous Consumer Access " and should be changed from the default setting of “enabled” to “trusted”.

Expert Assist Configuration—Audio and Video Hold Treatment

Note: In Remote Expert Co-browse, REAS is not responsible for the call, so this section can be ignored

You can configure how hold is rendered to endpoints using the settings in the `proxy.properties` file on each of the REMB servers. You can find this file at `/opt/cisco/<release-number>/CSDK/media_broker/`. You can configure several properties with the main ones listed below, whether or not audio on hold is enabled:

- `video.hold.on`
  - `true|false`
  - Whether or not video on hold is enabled
  - Default: `true`
- `video.hold.image.path`
  - Video hold image path—image must be in PNG format
  - Default: `./resources/hold.png`
- `audio.hold.on`
  - `true|false`
  - Whether or not audio on hold is enabled
  - Default: `true`

Note: The `proxy.properties` file is not replicated between Media Broker instances, so must be updated on each instance.

Expert Assist Configuration—Call Admission Control

Note: In Remote Expert Co-browse, REAS is not responsible for the call, so this section can be ignored

Call Admission Control is designed to "protect" Media Broker component against overloading when one is being selected to handle a new call. It can be configured as follows:

1. Log into the RE Mobile Web Administration Console `https://<Cluster IP or FQDN>:8443/web_plugin_framework/webcontroller` using the credentials you configured when you ran the **setup.sh** script..
2. Navigate to the **Gateway** tab and click the **General Administration** menu.
3. Change the setting as required.
   Note: Call Admission Control is disabled by default (set to '0'), with a Max Load Factor of '75'.

With Call Admission Control being enabled, if a Media Broker is deemed unable to handle another call, the Remote Expert Mobile Application Server will attempt to select another Media Broker—this, of course, introduces the risk that a new call will be rejected due to no Media Brokers being available.

The following are configurable fields:

Max Load Factor	The maximum Media Broker load limit. When a call is assigned to a particular Media Broker, the Media Broker will reject the call if its current load factor is at, or above, this value—this will cause the Remote Expert Mobile Application Server to choose another Media Broker (if one is available). **Note:** A value of "0" in this field will disable this function, that is, no check will be made

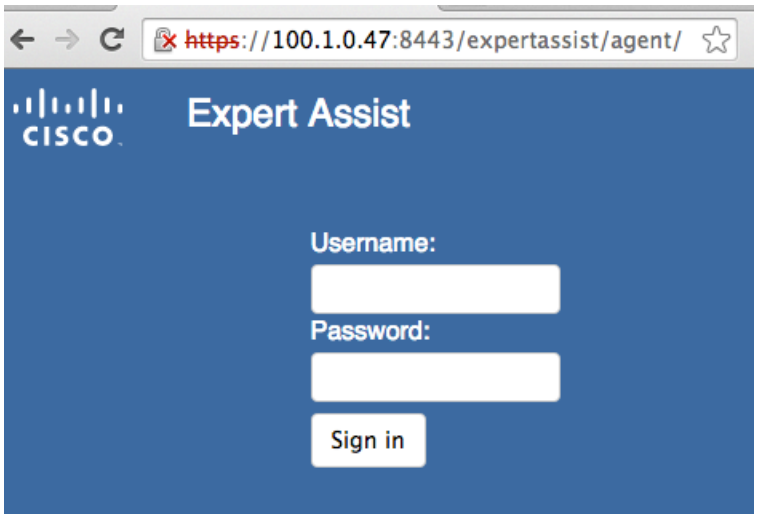
SDP Control Request Timeout	The maximum number of milliseconds to wait for SDP control requests to complete between the Remote Expert Mobile Application Server and Media Brokers. If the request does not complete within this timeout period, the Remote Expert Mobile Application Server will try another Media Broker.If all MBs are overloaded then the call is immediately rejected.

Post-Install Verification

Once you have completed deployment of the RE Mobile cluster, it is recommended that you verify that the solution is properly configured. This may be done without the use of any additional network components (such as Cisco Contact Centre or CUCM). This verification makes use of the Expert Assist Agent Console and the sample consumer application—these are explained in more detail in later sections but for now we will just make use of them to make a test Expert Assist call and co-browse session.

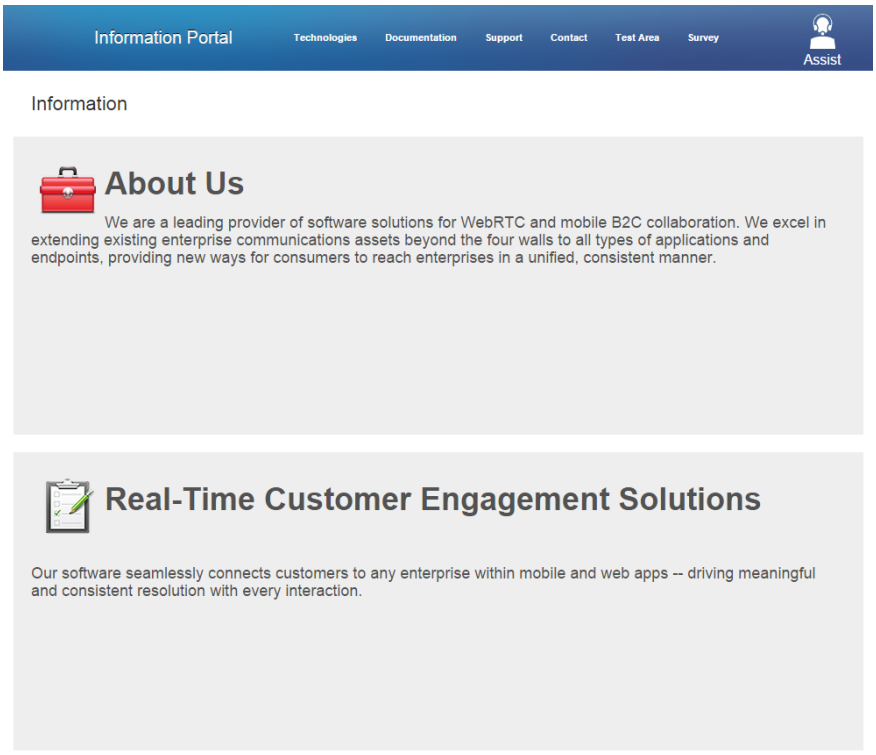
Using a Call

1. From a browser window, log into the Agent Console
    a. For the agent application, open an incognito browser window within Chrome from a system with a webcam
    b. Navigate to: `https://<Cluster IP or FQDN>:8443/expertassist/agent`



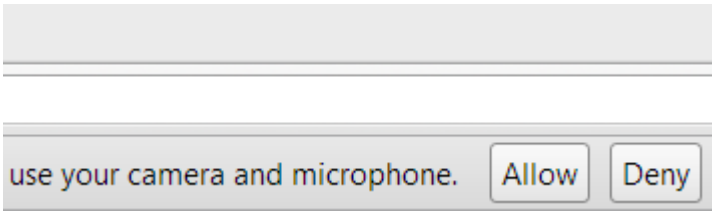
    c. Enter the following credentials:
        - Username: **agent1**
        - Password: **agent1**
          You will now be logged in as an agent
2. From a separate machine to the one used above, or an “Incognito” window if Chrome was used, navigate to the consumer sample application.

a. Navigate to https://<Cluster IP or FQDN>:8443/assistsample



b. Begin an Assist session by clicking the Assist button in the upper right of the screen.

c. Click to allow your browser access to your microphone and webcam.



3. A call will arrive at the agent console, click to answer the call.
There should now be a voice and video call established between the consumer and agent.

Testing Remote Expert Co-browse

This test can also be performed with the full version of Expert Assist; it is the only test which can be performed with Remote Expert Co-browse.

1. From a browser window, log into the Agent Console by navigating to https://<Cluster IP or FQDN>:8443/expertassist/agent?cid=sharedid
2. From a separate machine or an incognito window, navigate to https://<Cluster IP or FQDN>:8443/assistsample?cid=sharedid&cobrowseOnly=true
3. Click the Assist button to the top right to start a co-browsing session
4. Select the drawing tool on the Agent desktop, and draw on the shared view. The annotations should appear on the consumer screen as well.

5. Test the other Expert Assist tools in the same way.

Changing Passwords

Changing the Administrator Password

Note:

- If the Expert Assist Administration credentials have been forgotten or locked, see the section Resetting Expert Assist Administrator Credentials on page 55.
- Do *not* use the `setup.sh` script to change user credentials or passwords after installation; use the `change-passwords.sh` script, as described below.

Password length:

Passwords must be between 4 and 100 characters long.

On the master REAS:

Important: If the REAS password is updated on the master, the script must then be run on all slaves to reflect the updated REAS password—otherwise the cluster will become out of operational sync, and slave upgrades will fail.

1. SSH in to the operating system as the **rem-ssh** user, then use `su` to change to the **rem-admin** user.
2. Run the following script:

   ```
   /opt/cisco/bin/change-passwords.sh
   ```

3. Follow the prompts to reset the following passwords—to leave a password unchanged, leave the password field blank then press the **Enter** key to move onto the prompt for the next password:
   - Expert Admin Assist—The Expert Assist Admin credentials are used for authenticating user access to both the REM Web Admin Console and the REAS Management Console. The default username is `administrator`.
   - Remote Expert AS master/slave—The Remote Expert AS master/slave credentials are used for authenticating access to the master node from any slave nodes (that is, this not for user access)—they are used for internal communications between the REAS elements within the cluster only, and not by administrators. The same master/slave credentials need to be used across all REAS nodes in the cluster. The default username is `master`. **Note:** The username and password cannot be identical to each other.

   Important: After running this script on the master REAS node, be sure to run it on *all* slave nodes.

On all slave REAS nodes:

Note: On the REAS slave, the script allows you to update the slave about the new master REAS password—running the script on the slave does not prompt for the Expert Assist Administration password.

1. SSH in to the operating system as the **rem-ssh** user, then use `su` to change to the **rem-admin** user.
2. Run the following script:

   ```
   /opt/cisco/bin/change-passwords.sh
   ```

3. Follow the prompt to enter the password already set on the REAS master—this is to enable the slave to stay in operational sync with the REAS master.

On the REMB:

Note: In Remote Expert Co-browse, there is no REMB, so this section can be ignored

On the REMB, the REAS and Expert Assist passwords are not relevant, and therefore cannot be set.

Changing the KeyStore Password

To change the default KeyStore password on the REAS, perform the following steps:

1. Log into the REAS Management Console `https://<Cluster IP or FQDN>:9990`
2. In the REAS Management Console, from the top-right menu select **Profiles**.
3. From the **Profile** drop-down list, select the **management** profile.
4. From the menu on the left, expand **Subsystems > Trust Management > ID Certificates**.
   The top part of the page shows the following identity certificate groups that map to the clustered KeyStores:
   - **loadbalancer**
   - **main**
   - **management**
5. Choose the **loadbalancer** KeyStore to change its password, then click **Change Password**.
   This displays a pop-up—enter appropriate values for the current password and new password, then click **Save**.

   Note: The certificate KeyStore password defaults to `changeit`.

Changing the TrustStore Password

To change the default TrustStore passwords on the REAS, perform the following steps:

1. Log into the REAS Management Console `https://<Cluster IP or FQDN>:9990`
2. In the REAS Management Console, from the top-right menu select **Profiles**.
3. From the **Profile** drop-down list, select the **management** profile.
4. From the menu on the left, expand **Subsystems > Trust Management > Trust Certificates**.
5. Choose the **default-trust** trust group to change its password, then click **Change Password**.
   This displays a pop-up—enter appropriate values for the current password and new password, then click **Save**.

   Note: The certificate TrustStore password defaults to `changeit`.

Resetting Passwords

Resetting Expert Assist Administrator Credentials

If the Expert Assist Administration Portal username and/or password have been forgotten or locked, then they can be reset to the defaults by setting a system property, which will reset the credentials on the next login attempt.

To Reset Expert Assist Administrator Credentials

1. Log in to the REAS Management Console `https://<Cluster IP or FQDN>:9990`
2. In the REAS Management Console, from the top right menu, select **Server**.
3. From the menu on the left, click **Server > Server Groups**.
   The Server Groups page displays:
4. In the **Available Group Configurations** list, select **main-server-group**.
5. Add a new system property—select the **System Properties** tab and click **Add**.
   The **Create System Property** dialog displays.
6. In the **Name** field, enter `appserver.admin.password.reset`
7. In the **Value** field, enter `true`
8. Click **Save**.
   Login is now disabled on the Expert Assist web administrative interface and the next login attempt, regardless of the credentials entered, will reset the credentials to the defaults (Username: administrator, Password: administrator) and reset the failed login counter to zero.
9. Open a new web browser and log into the RE Mobile Web Administration Console
   `https://<Cluster IP or FQDN>:8443/web_plugin_framework/webcontroller`
   using the credentials you configured when you ran the **setup.sh** script.
10. In your REAS Management Console window click **Remove** in the row containing the system property `appserver.admin.password.reset`
11. Restart REAS master
    Login is now re-enabled on the web administrative interface and the credentials are reset to the default values.
    Note: Change the default log-in details after the first login—see Changing the Administrator Password on page 53.

Resetting REAS Administrator Credentials

To reset the REAS Admin Console credentials, run the `change-passwords.sh` script—see Changing the Administrator Password on page 53.

Integrating Remote Expert Mobile

If you have successfully run the post-install verification test call, then you now have a working Remote Expert Mobile installation. This section will take you through the steps required to integrate with your wider Cisco environment. RE Mobile can be integrated into either a Unified Communications or Contact Center infrastructure, see the *Cisco Remote Expert Mobile—Design Guide* for more information. The following section describes how to configure these other elements to work with RE Mobile in these infrastructures.

General configuration for RE Mobile integration into Unified Communications or Contact Center Environments

The following configuration must be performed whether you are integrating into a UC or CC environment.

1. Log into the RE Mobile Web Administration Console
   `https://<Cluster IP or FQDN>:8443/web_plugin_framework/webcontroller`
   using the credentials you configured when you ran the **setup.sh** script.

2. Navigate to the Agent Consoles tab and click the Agent Consoles Administration menu.

   This interface allows the configuration of the following:

   - Expert Assist Agent Name Label
     - Enabling the '**Display Agent Name**' property causes the Agent's name to be displayed to the consumer when the call is established.
       - For UC integrations this will be the '**First Name**' field (configured in Cisco Call Manager)
       - For CC integrations this will be the agent name as configured in Finesse User's name.
     - If a specific label is required to be displayed to the consumer when the Expert Assist call is established in place of the Agent's name, the '**Display Agent Name**' property should be disabled. Additionally, a value should be entered in the '**Fixed Agent Name**' field representing the required label to be used.
   - Outbound HTTP Proxy Setting
     - This property should only be filled in if Finesse Agents using the gadget will be sharing documents hosted externally that require access via a HTTP proxy. Otherwise, it should be left blank.
     - The format of this property is: http://proxyserver:port
   - Certificates Settings
     - The '**Trust All Certificates**' property defines whether or not to trust **ALL** HTTPS certificates provided by the remote server when making outbound connections, for example.

       When the Agent gadget requests access of documents over HTTPS,

       When Expert Assist communicates with the Cisco Call Manager via its AXL interface.
     - The '**Trust JDK Certificates**' property defines whether or not to trust those HTTPS certificates defined within the default JDK trust store (i.e. those certificates signed by 'well-known' CAs) when making outbound connections, for example.

       When the Agent gadget requests access of documents over HTTPS,

       When Expert Assist communicates with the Cisco Call Manager via its AXL interface.
   - Local User Authentication
     - These properties allow a 'local' Expert Assist user to be defined with the Agent and/or Supervisor role—*The spelling and case sensitivity of these roles is extremely important.*

- It is enabled by default for a fresh installation, the username and password are set to **agent1**. This default user can only log in to the Expert Assist Console.
  Consider disabling this local user for production deployments.

- When a user logs in using the Expert Assist Console or Finesse Agent Console, their credentials are first compared to those of the configured 'local' Expert Assist user. If the credentials match, the role assigned to the 'local' user will determine whether the user will have access to the Agent and/or Supervisor consoles or gadgets. If the credentials do not match the local user, then normal Finesse/AXL authentication will take place.

- A list of Finesse Servers

  This configuration is relevant only to Contact Center deployments

  - REAS uses this list of servers to authenticate both Agents and Supervisors that are using the Finesse gadgets.

    When a user initiates an action (either the Supervisor gadget loading the resources that will be shared between agent and consumer, during its initialization process; or the Agent gadget requesting the consumer's permission to start a screen-share session), the RE Mobile Finesse gadget requests permission from Expert Assist to allow that user to perform the action.

    As part of this request, the gadget sends the user's Finesse credentials to Expert Assist, along with the name of the Finesse server that the user is connected to.

    Expert Assist then attempts to contact that Finesse Server (verifying that it is in the list of servers), and asks it to validate the user's role. This allows multiple Peripheral Gateways (PGs) to work with a single REAS cluster.

  - Click the **Add** button and enter the HTTP(S) URL of each Finesse Server (for example, **https://<FinesseAddress>:<Port>**).

  - As Finesse is being accessed securely, the appropriate Certificate Settings (see above) must be selected.

- Call Manager Settings

  This configuration is relevant only to Unified Communications deployments.

  - Users logging into the Expert Assist Agent or Supervisor Consoles are authenticated against CUCM using the AXL interface. Those users must have particular roles in order to be given access to the consoles—see the *Cisco Remote Expert Mobile—Expert Assist Web Agent and Supervisor Consoles User Guide* for more details.

  - Click the **Add** button and enter the HTTP(S) URL of each Call Manager (for example, **https://<CMAddress>:<Port>**). Then click **Submit**.

  - Enter the username and password for a CM user with permission to query user details over the AXL interface.

  - RE Mobile can be used in one of two ways—with Finesse integration or without (also known as the UC deployment model). In both cases, the customer dials into a single number, which is then routed to an available agent. See Integrating RE Mobile into a Unified Communications Environment on page 59

  - In the UC deployment model, as RE Mobile does not have the ability to configure hunt groups, we use the UCM Extend and Connect feature for this. This means that the customer still targets a single DN which will be configured on the UCM as a hunt group (also known as a hunt pilot) number. This then sends the customer's call to the members of the group. Each of the members has a Remote Destination defined which matches a route pattern and sends the call to RE Mobile using a SIP trunk. All this UCM configuration (hunt pilot, remote destination, and route patterns) makes up the Extend and Connect feature in UCM.

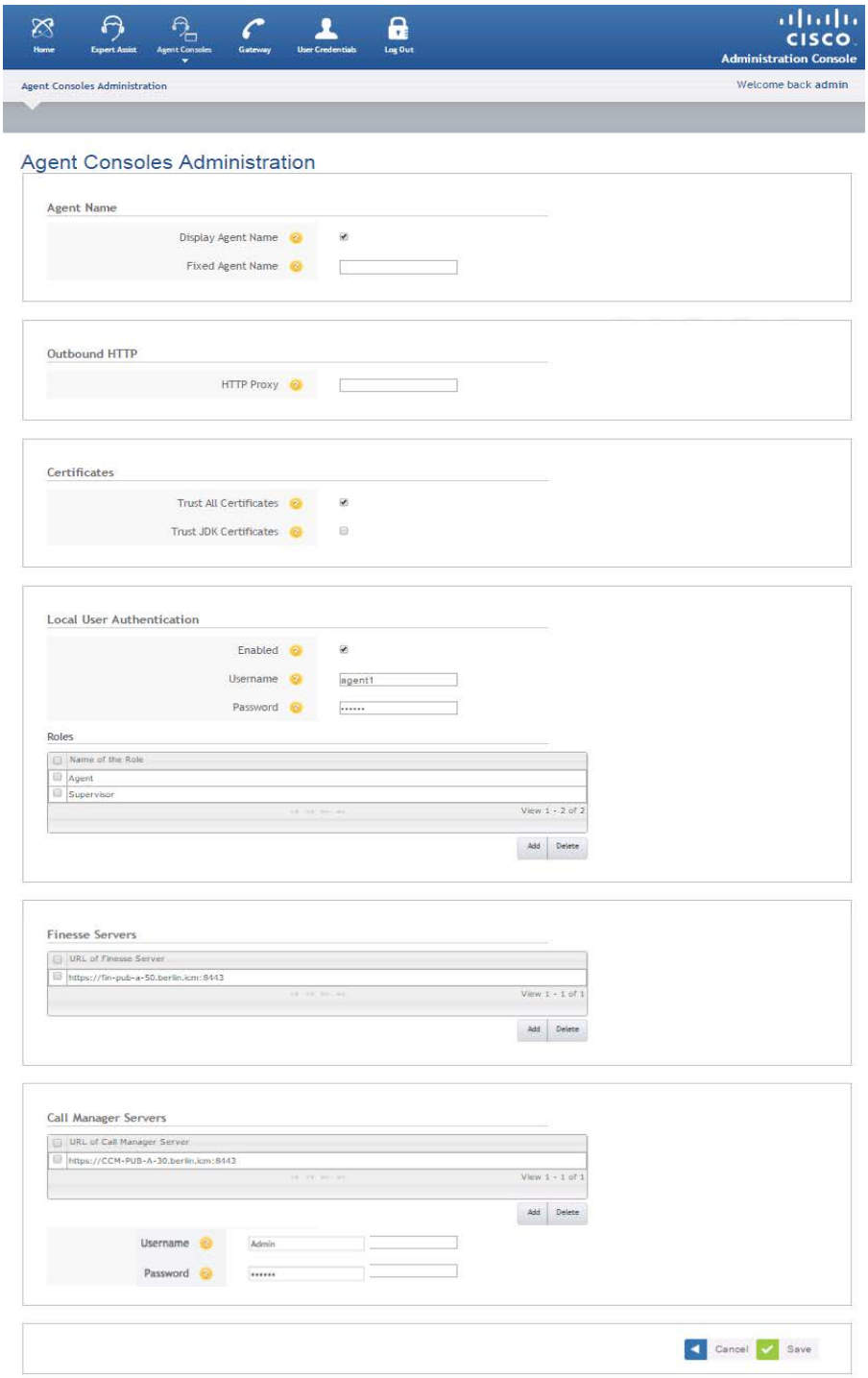
  - In RE Mobile, we have a number of agents signed in using the Expert Assist Agent Console waiting to receive the customer's call. REM uses the UCM AXL interface to validate the agent credentials when they login.

3. Click “**Save**” to persist the configuration changes.

   Note: RE Mobile authenticates against either Finesse Servers or CUCM (over AXL). There are a few approaches to ensuring these servers are trusted by the gadget

   - Set **Trust All Certificates** to true (only recommended for trials)
   - Set **Trust JDK Certificates** to true (this will only work if Finesse/AXL are signed by a well known CA) or
   - Install the Finesse/AXL identity certificates into the REAS 'assist' trust store.

   The screenshot below shows the layout of the properties described above on the Remote Expert Mobile Administration interface.



Integrating RE Mobile into a Unified Communications Environment

In a Unified Communications infrastructure, RE Mobile provides two web applications:

- Agent Console—allows screen share features between consumer and agent.
- Supervisor Console—allows screen share files and links to be managed.

See the *Cisco Remote Expert Mobile—Expert Assist Web Agent and Supervisor Consoles User Guide* for information on using these applications.

Configuration Steps

Task	Description
Configure Cisco Unified Border Element and Cisco Unified Communications Manager	See the *Cisco Remote Expert Mobile—Solution Configuration Guide* for details on configuring your environment to integrate with Remote Expert Mobile.
Configure Call Manager address(es) for AXL authentication	Configure RE Mobile with the addresses of the Call Managers in order for RE Mobile to authenticate agents and supervisors using the console(s). See “General configuration for RE Mobile integration into Unified Communications or Contact Center Environments” above
Configure outbound SIP routing	RE Mobile needs to route calls to CUBE/CUCM. See “RE Mobile Gateway Configuration—Outbound SIP Server” above for details on how to configure this.
Test	See “Testing the Agent Console” below.
Inbound calling restrictions (optional)	Optionally, configure Expert Assist to limit URIs that the consumer can dial—See the “Expert Assist Configuration—Consumer Access Number Regex” section above for details.

Configuring a UC Deployment

1. Set up the agents in CUCM administration as "End Users".
    - The user id should match the remote destination name below (for example, 8000). This is because the user id and password are used to log in to the REM Expert Agent Console and the agent only receives calls that match this user id.
    - The user must be assigned the role "Standard CCM End User"
2. Configure each Agent with a phone as follows:
    - Phone type—CTI Remote device
    - Remote destination—Unique number (for example, 8000) with the extend and connect option checked
    - Line/directory number—Unique number (for example, 9000)
3. Direct Extend and Connect calls to the REAS server:
    - Create a SIP trunk for the REAS cluster. Add a destination to this trunk for each REAS server in the cluster.
    - Add a route pattern (for example, 80XX) which uses the REAS trunk above.
4. When you have configured all the end users, set up a hunt pilot, hunt list, and line group to represent this group of agents.
    - The hunt pilot defines the extension (for example, 5100) that the group can be dialed on and is configured with the hunt list
    - Associate the hunt list with one or more line groups
    - Associate the line group with a list of directory numbers to ring. In the RE Mobile UC deployment model, each of the directory numbers will be associated with an extend and connect remote destination through the agent's "CTI Remote Device" (see above).

5. The sip connectivity between the RE Mobile server and CUCM is typically done through CUBE or CUCM.

6. On the REM side, the following configuration is required. Log into the RE Mobile Web Administration Console `https://<Cluster IP or FQDN>:8443/web_plugin_framework/webcontroller` using the credentials you configured when you ran the **setup.sh** script.

    a. Configure the "Gateway > General Administration > Outbound SIP Server" to be "sip:<IP address of CUBE, or CUCM for CCX and UC deployments>

    b. Configure the "Agent Consoles > Agent Consoles Administration"

    c. Call Manager Servers: https://<IP address and port of CUCM>

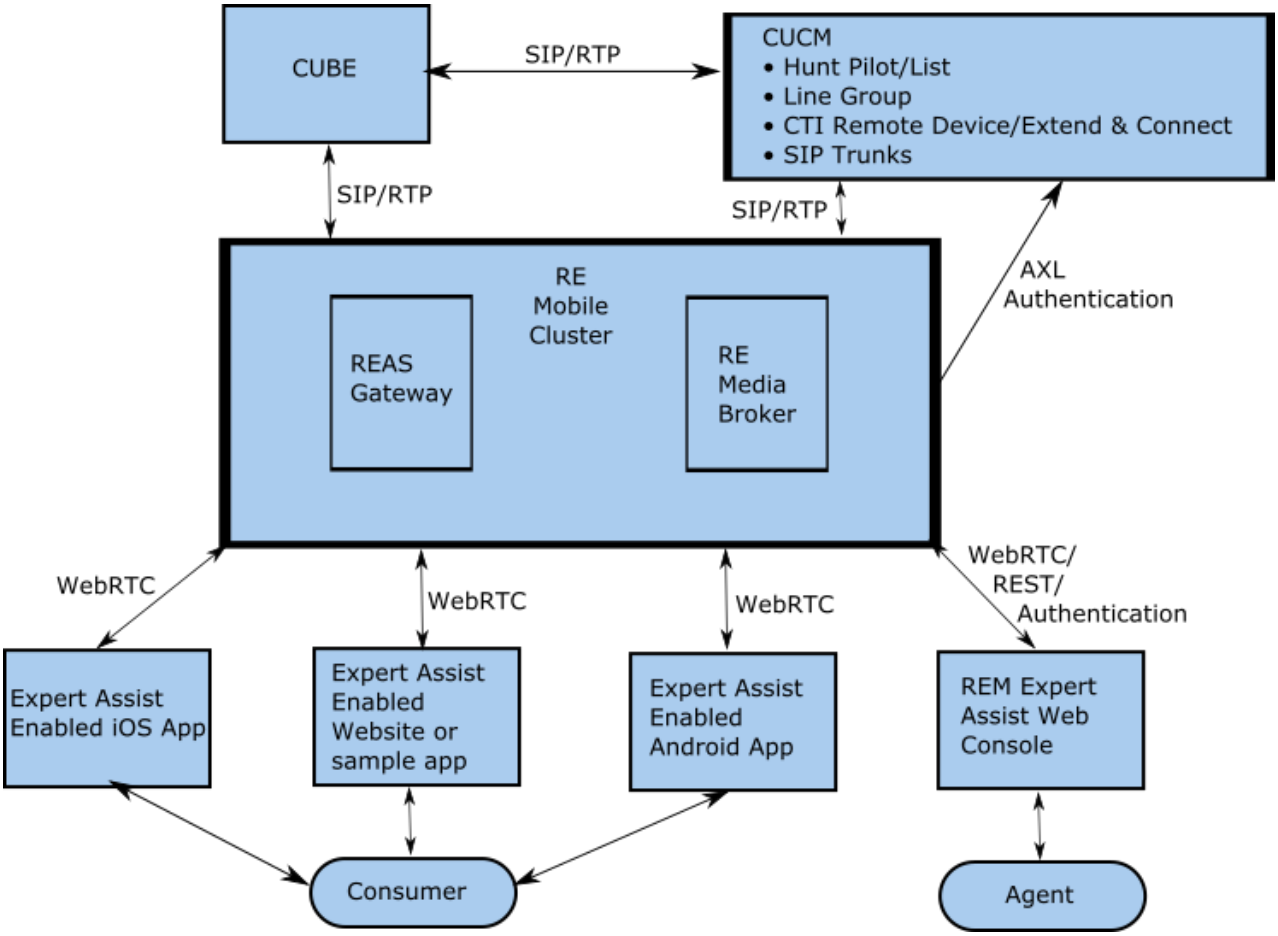
    d. Call Manager Username: for example, Admin, Call Manager Password: *****

    Note: If Call Manager Server URL above is HTTPS but does not have a valid certificate, then it will be necessary to either check the **Trust all certificates** option, or to add the certificate to the REAS 'assist' trust store.

7. Configure the CUBE with appropriate dial-peer to allow consumer calls from REAS to the hunt group (for example, 5100).

UC Deployment Model

Note: In Remote Expert Co-browse, REAS is not responsible for the call itself, so only the WebRTC communication between Consumer, Agent, and REAS are relevant.



A call takes the following route:

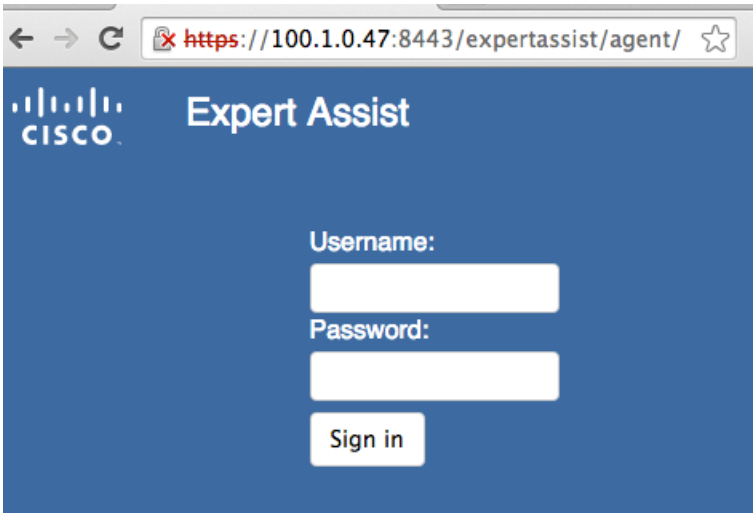
1. Consumer visits consumer web page, for example sample app at the following URL: `https://<Cluster IP or FQDN>:8443/assistsample/?agent=sip:5100@foo.com`
2. Consumer clicks the Assist button to initiate a call.
3. The REAS routes the call to its outbound SIP server (CUBE or CUCM, whichever is configured).
4. The dial-peer in the CUBE sends the call to CUCM. If using a no-CUBE deployment, the call directly reaches CUCM as in the outbound SIP server configuration.
5. CUCM hunt pilot matches the 5100 extension and a directory number (for example 9000) is selected from the line group. The agent associated with directory number has his remote destination (8000) called.
6. CUCM forwards the call to REAS because the trunk route pattern (80XX) matches.
7. REAS receives the call and delivers call to an agent that has logged in as 8000 at the following URL: `https://<Cluster IP or FQDN>:8443/expertassist/agent`

Testing the UC Integration

Note: In Remote Expert Co-browse, REAS is not responsible for the call, so the integration cannot be tested in this way. You will need to test the actual application which uses Expert Assist in co-browse only mode.

The following steps illustrate how to test that RE Mobile has been properly installed and configured for integration with CUCM/CUBE:

1. Ensure an agent is logged in to the Agent Console.
   a. Navigate to: `https://<Cluster IP or FQDN>:8443/expertassist/agent`



   b. Enter the credentials of an end user with the “Standard CCM End Users” role
   c. You should now be logged in as an agent
2. A consumer should browse to any Remote Expert Mobile Assist enabled website (this may be the sample website installed with the product).

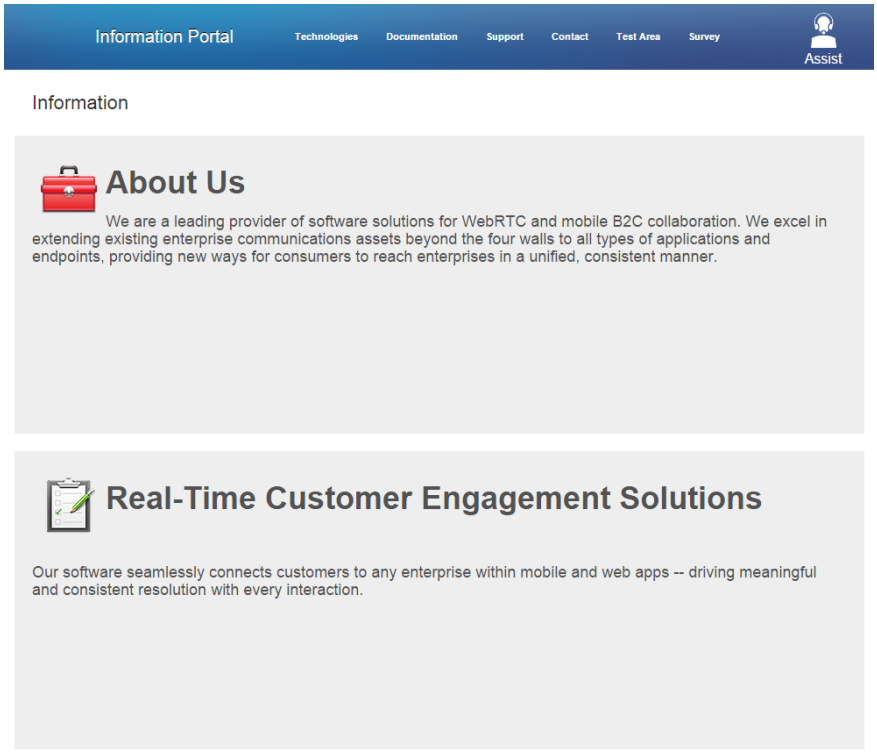
   If using the sample website:

   Navigate to the website URL, providing the agent details as a URI encoded parameter. The URL should take the form:

   https://<rem-server-address>/assistsample/?agent=sip:<tel-number>@<CUBE__OR_CUCM_IP>

For example, if the RE Mobile server address is example.com, and the agent URI is `sip:60017@100.1.0.100` (where 100.1.0.100 is the IP address of the Cisco UBE):

https://example.com/assistsample/?agent=sip:60017@100.1.0.100



Note: The Agent and Consumer pages **must** be opened on separate machines, or different browsers, or in Chrome's Incognito mode to avoid web socket issues. These issues will only arise during testing.

3. Click on the Assist button.

   A call will arrive at the agent console.

4. Click Answer in the agent console.

   A two-way voice/video call is established

Integrating RE Mobile into a Contact Center Environment

In a Contact Center infrastructure, RE Mobile provides two Finesse Gadgets:

- Agent Gadget—allows screen share features between consumer and agent.
- Supervisor Gadget—allows screen share files and links to be managed.

For more information on using these gadgets, see the *Cisco Remote Expert Mobile—Finesse Agent and Supervisor Gadget User Guide*.

Configuration Steps

Task	Description
Configure inbound calling	See the *Cisco Remote Expert Mobile—Solution Configuration Guide* for details on configuring your environment to integrate with Remote Expert Mobile. You will need to: • Configure an inbound number must be defined allowing RE Mobile consumers to call into Agents. • Configure CCE/CCX to route the configured inbound number to one or more Agent queues.
Finesse Server Trust Management	Enable HTTPS communication from the Finesse Server(s) to the REAS—See Finesse Server Trust Management on page 65.
Configure gadgets in Finesse	Configure the Cisco Finesse Administration web application with the location of the RE Mobile cluster hosting the Agent and Supervisor Gadgets—See the Configuring the Agent and Supervisor Consoles within the Finesse Server section on page 66 for details.
Configure RE Mobile with Finesse Server Addresses for authentication	Configure the addresses of the machines within the Finesse server cluster via the Web Gateway's administration console.
Configure outbound SIP routing	RE Mobile will route SIP messages via one or more CUBEs. See RE Mobile Gateway Configuration—Outbound SIP Server on page 42 for more information on how to configure these addresses
Enable SSLv2Hello (pre 10.6 Finesse)	Enable SSLv2Hello on REAS when integrating with Finesse Server versions prior to 10.6—See the Enable SSLv2Hello Support section on page 65 for details.
Test	See Testing the CC Integration on page 68.
Inbound calling restrictions (optional)	Optionally, configure Expert Assist to limit URIs that the consumer can dial— See Expert Assist Configuration—Consumer Access Number Regex on page 46.

Enable SSLv2Hello Support

Note: Versions of Cisco Finesse before 10.6 make gadget requests using SSLv2Hello protocol. SSLv2Hello is disabled by default within RE Mobile due to the POODLE vulnerability (October 2014).

A script has been included with the RE Mobile OVA that will enable support for SSLV2Hello. To enable legacy SSLv2Hello, invoke the **<REAS_INSTALL_DIR>/resources/enable-sslv2.sh** script on the master REAS host, and then restart the service. Once it has been restarted, the script must be executed on all the slave nodes within the cluster, for example,

```
[root@reas-master ~]# /opt/cisco/<REAS_INSTALL_DIR>/resources/enable-sslv2.sh
```

And to return to default behavior, invoke the **<REAS_INSTALL_DIR>/resources/disable-sslv2.sh** script on each REAS host in the cluster, for example.

```
[root@reas-master ~]# /opt/cisco/<REAS_INSTALL_DIR>/resources/disable-sslv2.sh
```

Finesse Server Trust Management

To provide a secure Finesse Desktop, the HTTPS identity certificate of the cluster hosting the Expert Assist Gadgets must be added to the Finesse Tomcat trust-store.

The following steps describe how to achieve this:

1. Obtain the REAS certificate
   - Follow the Exporting an identity certificate section on page 40 to export the Load Balancer's HTTPS identity certificate.

     Note: Ensure to select the **main-loadbalancer-group** identity certificate group, and then its **https** identity certificate.
2. Add the REAS certificate Finesse's Tomcat trust-store
   - Refer to the "**Add Certificate for HTTPS Gadget**" section within the *Cisco Finesse—Administration Guide* for details:
     http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/finesse/finesse_1051/user/guide/CFIN_BK_C3A9BCBC_00_cisco-finesse-administration-guide-1051.pdf

     Note: The Tomcat service must be restarted on all the Finesse nodes after the certificate has been imported into Finesse.

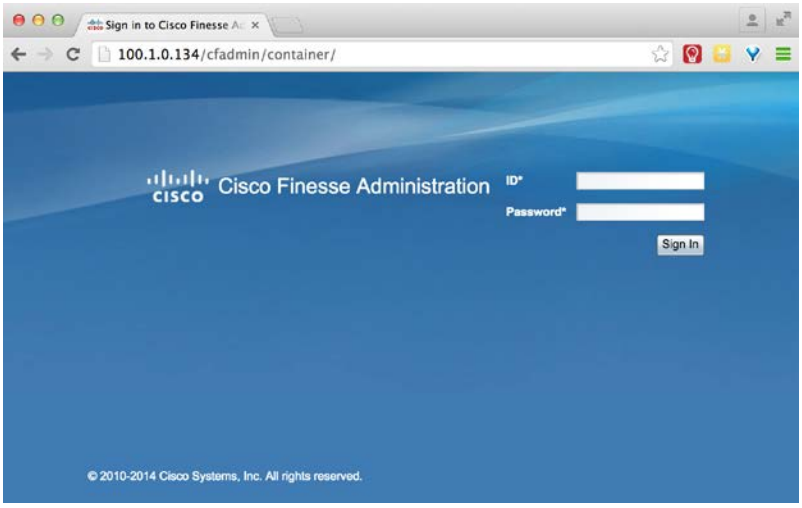
Configuring the Agent and Supervisor Consoles within the Finesse Server

The Finesse server needs to be configured with the location of the Expert Assist Agent and Supervisor Consoles.

The following steps explain how to achieve this.

1. Open the Cisco Finesse Administration web console by navigating to:

   https://<finesse-server>/cfadmin/container/



2. Enter the Administrator user's credentials and click 'Sign in'.
3. Navigate to the Desktop Layout tab.
4. Adding the Agent and Supervisor consoles to the Finesse console is achieved by editing its layout (defined in XML).

   The Finesse console's UI is divided into tabs. Each of these can contain one or more gadgets. The RE Mobile Agent and Supervisor gadgets will be configured to reside in separate tabs on the Finesse console.

   The XML layout of the Finesse console is separated into 2 sections as shown in the diagram below:

   One defining the content within the tabs that all Agents have access to

   And another defining the content within the tabs that all Supervisors have access to

```
…
<layout>
  <role>Agent</role>
  <tabs>
    <tab>
      Finesse Agent Gadget Definition
    </tab>
  </tabs>
</layout>

<layout>
  <role>Supervisor</role>
  <tabs>
    <tab>
      Finesse Supervisor Gadget Definition
    </tab>
  </tabs>
</layout>
```

Based on the diagram above, the XML required to define the Agent and Supervisor tabs in order to configure the appropriate Console is shown below.

Agent Console Definition

```
<tab>
  <id>EA</id>
  <label>Expert Assist</label>
  <gadgets>
    <gadget>https://<reas-address>:8443/finesse_assist_gadget/
FinesseAssist.xml?finesseVersion=11.5.1
</gadget>
  </gadgets>
</tab>
```

Note: Ensure that the `finesseVersion` request parameter in the URL above is modified to your version of Finesse. If a value of 11.5(1) or later is used, then Finesse assets (such as `finesse.js`) will be loaded from the Finesse server rather than the gadget. The change in where assets are loaded should improve compatibility of the gadget running in future versions of Finesse.

Supervisor Console Definition

```
<tab>
  <id>EAS</id>
  <label>Expert Assist Supervisor</label>
  <gadgets>
    <gadget>https://<reas-address>:8443/finesse_assist_admin_gadget/
FinesseAssist.xml?finesseVersion=11.5.1 </gadget>
  </gadgets>
</tab>
```

5. The XML above should be copied, edited and pasted into the appropriate section of the **Desktop Layout XML**.

   a. Replace the **reas-address** with either the IP address of the master REAS node, or the DNS resolvable REAS cluster-address.

      The example above shows the URL used to access the Gadgets (hosted on the REAS cluster) being secure. This may be changed to be insecure if required.

      If the URL is secure, the Finesse servers **MUST** be configured to trust the REAS cluster—See the "**Finesse Server Trust Management**" section above.

   b. Copy the Agent and Supervisor tab definitions into the appropriate section(s) of the console layout.

      Note that the Agent tab definition **MUST** be pasted into the "Agent" role section within the XML.

      However, it may also be pasted into the "Supervisor" role section if all Supervisors were to require Agent functionality.

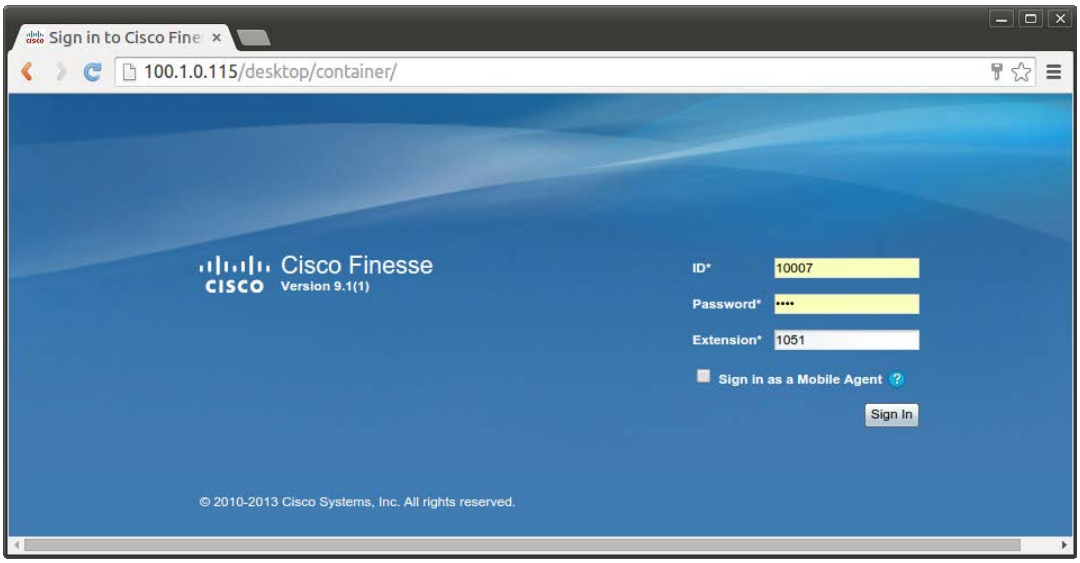
   c. Click **Save**.

Testing the CC Integration

The following steps illustrate how to test that the Finesse Gadget has been properly installed and configured:

1. Ensure a Finesse agent is logged in to the Finesse Server.

   a. Navigate to https://<finesse-server>/desktop/container/



   b. Authenticate with the agent ID, password and phone extension.

2. A consumer should browse to any Remote Expert Mobile Assist enabled website (this may be the sample website installed with the product).

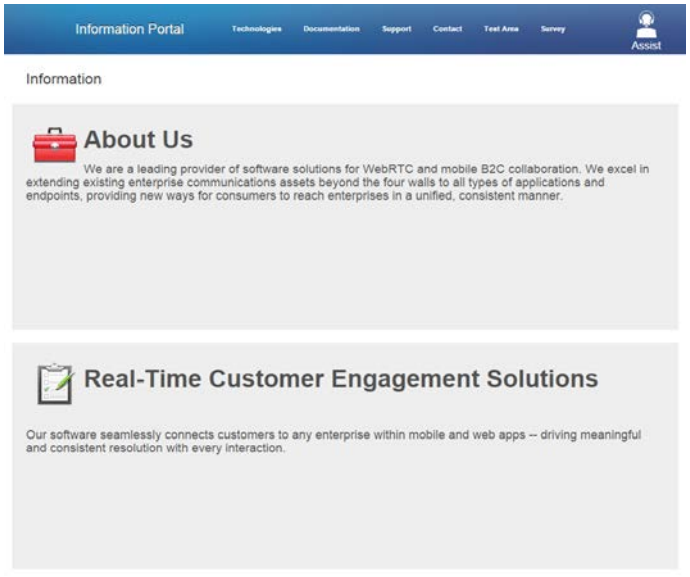
   If using the sample website:

   Navigate to the website URL, providing the agent details as a URI encoded parameter. The URL should take the form:

   https://<rem-server-address>/assistsample/?agent=sip:<tel-number>@<CUBE_IP>

   For example, if the RE Mobile server address is example.com, and the agent URI is `sip:60017@100.1.0.100` (where 100.1.0.100 is the IP address of the Cisco UBE):

   https://example.com/assistsample/?agent=sip:60017@100.1.0.100



Note: The Agent and Consumer pages **must** be opened on separate machines, or different browsers or in incognito mode to avoid web socket issues. These issues will only arise during testing.

3. Click on the Assist button.

   A call will arrive at the agent console.

4. Click Answer in the agent console.

   A two-way voice/video call is established

Restricting Application URIs via the Reverse Proxy

The reverse proxy is installed in front of the REAS. Only making specific REAS URIs publicly visible results in clients (in the Consumer Network) only having access to the server resources they need, while all others are protected.

The following table shows the URIs that should be allowed through the reverse proxy.

Path	Protocol	Description
/csdk-sample/*	HTTP(s)	Client SDK sample application.
/gateway/csdk-sdk.js	HTTP(s)	Web SDK assets.
/gateway/csdk-aed.js	HTTP(s)	Web SDK assets.
/gateway/csdk-common.js	HTTP(s)	Web SDK assets.
/assistserver/defaultUIResources/*	HTTP(s)	Default UI used by iOS clients.
/assistserver/img/*	HTTP(s)	Some common graphical resources.
/assistserver/consumer	HTTP(s)	Servlet used to provide clients with a session.
/assistserver/sdk/web/consumer/*	HTTP(s)	Web SDK assets.
/assistserver/sdk/web/shared/*	HTTP(s)	Web SDK assets.
/gateway/adapter.js	HTTP(s)	Web SDK assets.
/assistserver/topic	Web Socket	WebSocket used for screen share, annotations …etc.
/gateway/websocketcall	Web Socket	Web Socket used for call control.
<web_gateway_host>:<web_gateway_port>/gateway/ie/*	HTTP(s)	Internet Explorer plug-in download
<web_gateway_host>:<web_gateway_port>/gateway/SafariPlugin/*	HTTP(s)	Safari plug-in download

The following specifically relates to the RE Mobile consumer-side sample application URIs.

Path	Protocol	Description
/assistsample/*	HTTP(s)	Expert Assist sample client application.

The following specifically relates to the URIs used by the RE Mobile Agent and Supervisor consoles.

Path	Protocol	Description
/expertassist/agent/*	HTTP(s)	Expert Assist Agent console.
/expertassist/supervisor/*	HTTP(s)	Expert Assist Supervisor console.
/gateway/adapter.js	HTTP(s)	Web SDK assets.
/assistserver/sdk/web/shared/*	HTTP(s)	Web Agent SDK assets.
/assistserver/sdk/web/agent/*	HTTP(s)	Web Agent SDK assets.
/gateway/csdk-phone.js	HTTP(s)	Web SDK assets.
/gateway/csdk-aed.js	HTTP(s)	Web SDK assets.
/gateway/csdk-common.js	HTTP(s)	Web SDK assets.
/expertassist/agent/token	HTTP(s)	Servlet used to provide Agents with a session.
/assistserver/topic/*	Web Socket	Web socket used by Agent to connect to a Consumer's screen share.

Dynamic Codecs

Note: In Remote Expert Co-browse, Dynamic Codecs is not used, so this section can be ignored

During the install process, REMB is provisioned with a temporary certificate that it can use for testing purposes if a reverse proxy does not terminate the secure WebSocket. The CN (Common Name) of the certificate reflects the cluster address specified during installation, which defaults to the server's IP address, but this could have been changed.

A common private Certificate Authority (CA) is used to sign the temporary certificate along with those that are installed by default with the AS cluster that the Gateway is installed to; this means that browsers do not automatically trust the certificate that the Media Broker defaults to. For testing when using this certificate, visit the WSS URI(s) configured for calls (see MOWS Clients on page 71MOWS ClientsMOWS Clients)—replace `wss://` with `https://` to be able to accept the certificate each time that the browser is opened. Replace the temporary certificate with a certificate signed by a third-party trusted CA to avoid the need to accept the certificate every time.

Media Broker uses a Java keystore to manage its certificates—for Dynamic Codecs, this is accessed using the "media-over-websockets" alias. See the following commands to generate a Certificate Signing Request (CSR) in order to get a certificate signed by a third-party trusted CA; then import that certificate into the newly created Java keystore.

1. Create a new keystore

   ```
   keytool -genkey -alias media-over-websockets -keyalg RSA -keysize 2048 -keystore
   yourdomain.jks
   ```

2. Generate a CSR (during this step the CN must be the FQDN used in the WSS URI configured for the media broker(s) media over websocket ports.

   ```
   keytool -certreq -alias media-over-websockets -keyalg RSA -file yourdomain.csr -keystore
   yourdomain.jks
   ```

3. Send the CSR to a CA for signing

   The procedure for getting your certificate signed by a third-party CA depends upon the requirements of that CA—see the guidance from the CA. You will require the file yourdomain.csr generated in the previous step.

4. Import the CA certificate into the client keystore.

   ```
   keytool -import -keystore yourdomain.jks -file ca-certificate.pem.txt -alias rootCA
   ```

5. Import the signed certificate

   ```
   keytool –import –keystore yourdomain.jks –file client.cer –alias media-over-websockets
   ```

   The file is in <install_directory>/media_broker. If the fields are blank, then the Java keystore generated during installation is used. The password must be the same as that entered during the creation of the Java keystore. The path needs to be a full path rather than just a file name or relative path.

   Note: For more details on managing certificates, see Configuring REAS with identity certificates signed by a third-party CA on page 36.

MOWS Clients

MOWS Clients

The Media-Over-WebSockets (MOWS) client settings define the addresses and ports through which media using WebSockets will be received from the client application, allowing MOWS traffic to pass through any firewalls in the network, typically with no need for any firewall configuration changes. MOWS uses H.264, thus avoiding any need for transcoding.

The following details are required:

- **Public WSS URI**—This is the URI used by the client to connect to the public address of the Media broker, which will be appended with a unique identifier for the call.
  It must start with "wss://", then have the public hostname of the Media Broker or reverse proxy followed by the port that the client connects to. We recommend that for most public-facing installations you use port 443, in order to allow the most reliable traversal of intermediate proxies. This can then be followed by a path that allows a reverse proxy to identify the particular media broker to pass the traffic to; if you are not using a reverse proxy, do not include a path.

- **Local Address**—The address on which Media Broker will listen for MOWS connections; it should be the same as the address in the Public URI, unless a reverse proxy is in use.

- **Local Port**—The port on which Media Broker will listen for MOWS connections; it should be the same as the port in the Public URI, unless a reverse proxy is in use.

- **Locally Secure WebSocket**—Leave this checkbox checked, unless an unencrypted connection is used between a reverse proxy and the Media Broker. The client can only create a secure connection, so unchecking this checkbox is only useful if there is a reverse proxy that handles the encrypted connection.

MOWS traffic is not enabled by default—enable it using the checkbox in the General Administration screen. With Dynamic Codecs enabled, traffic from users of Chrome will use MOWS; traffic from users of other browsers that do not support Dynamic Codecs will use WebRTC.

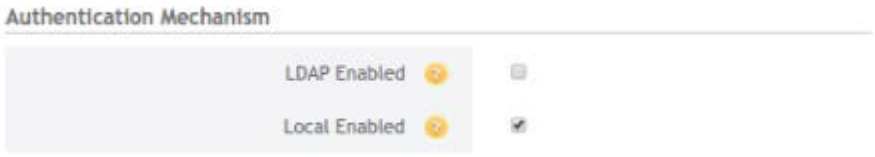
LDAP Authentication

Enabling LDAP Authentication

1. Log into the RE Mobile Web Administration Console
   https://<Cluster IP or FQDN>:8443/web_plugin_framework/webcontroller
   using the credentials you configured when you ran the **setup.sh** script

2. Under **Authentication Mechanism**, select either or both of the options as required, to enable LDAP or Local authentication.

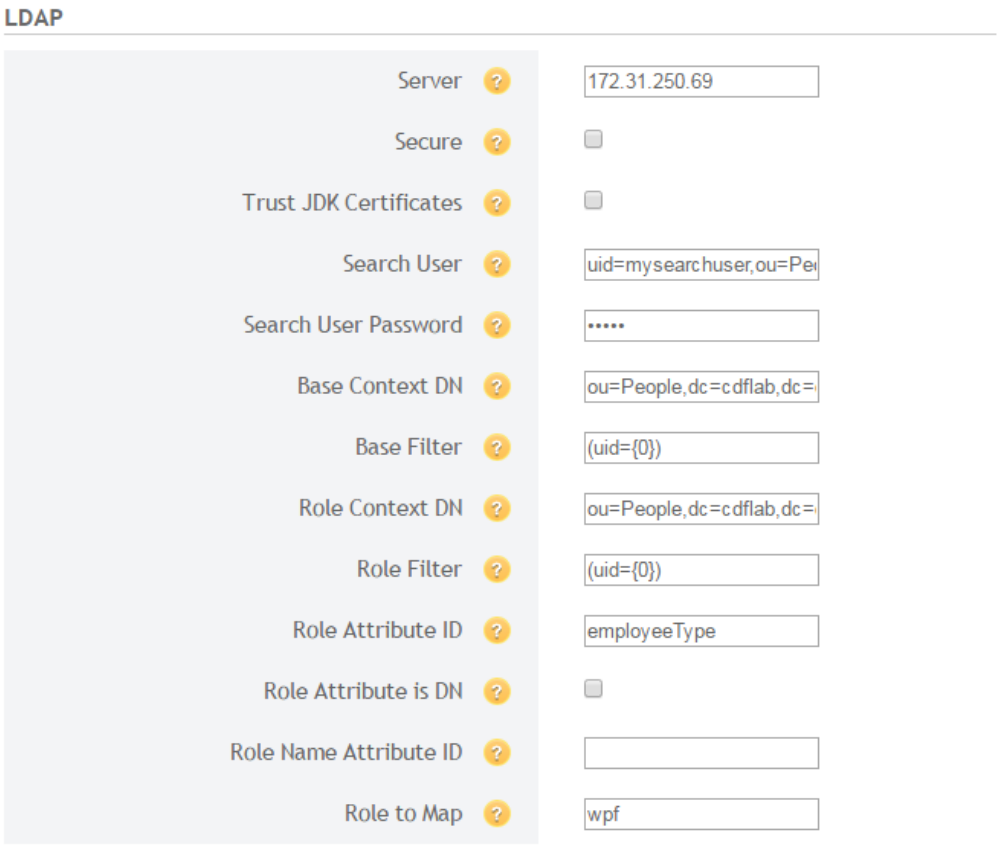
   Note: If both options are enabled, LDAP is done first, then (if necessary) Local.



Configuring LDAP Authentication

1. Log into the RE Mobile Web Administration Console
   https://<Cluster IP or FQDN>:8443/web_plugin_framework/webcontroller/credentials
   using the credentials you configured when you ran the **setup.sh** script.

2. Under **LDAP**, the following configuration settings are available:



Setting	Description
Server	The host of the LDAP server, for example 172.31.20.69
Secure	This checkbox indicates if LDAP authentication should be performed over a secure (HTTPS) connection. If checked, a valid LDAP server certificate needs to be imported. If unchecked, be aware that plain-text credentials are passed across the network.
Trust JDK Certificates	This checkbox indicates if, in addition to the regular LDAP trust store, the Java (JDK) default certificate trust store should be used for LDAP server certificate validation. If checked, the JDK trust store is used to validate an LDAP server certificate, if validation cannot be performed using the regular LDAP trust store. If unchecked, only the regular LDAP trust store will be used.
Search User	The full Distinguished Name (DN) of the user that will authenticate against the LDAP server and will be used to perform a search. An example is UID=SEARCHUSER,OU=USERS,DC=EXAMPLE,DC=COM
Search User Password	The password for the Search User
Base Context DN	This is the complete DN used to define the authentication parameters An example is OU=USERS,DC=EXAMPLE,DC=COM
Base Filter	The search filter syntax used in the authentication query. The input username will replace any {0} expressions. For example: In this search the filter is the user id. (uid={0}) This extra parameter will be attached to the existing query, for example: (UID={0}),OU=USERS,DC=FUSION,DC=VBOX
Role Context DN	The fixed DN of the context to search for user role by LDAP For example OU=Users,DC=ldap,DC=company,DC=com
Role Filter	This contains similar properties to the Base Filter but will be used in user role query.
Role Attribute ID	The name of the attribute of the role object that corresponds to the name of the role. For example employeeType

Setting	Description
Role Attribute is DN	This checkbox indicates whether the value of the attribute named by Role Attribute ID contains the fully distinguished name of a role object If checked, the value of the attribute named by Role Attribute ID represents the DN of a role object, in which case the role name is taken from the value of the Role Name Attribute ID attribute of the corresponding object If unchecked, the role name is taken from the Role To Map field
Role Name Attribute ID	The name of the attribute of the role object that corresponds to the name of the role. If Role Attribute is DN is checked, this property is used to find the role object's name attribute. If Role Attribute is DN is unchecked, this property is ignored,
Role to Map	The name of a user's role (as defined in LDAP) that authorises the user to access administrative capabilities. An example is wpf If blank, the user's role that REAS looks for when the Role to Map field is left blank is called: WEBADMIN

Important: If a user can log in to the REAS console using their LDAP credentials, but cannot see the administration pages after logging in, then check the **Role**-related configuration.

- LDAP authentication fails for first time user/user after reset
  If a user is set up in Active Directory with the option 'User must change password at next logon', but their first action as an AD user is to attempt to use LDAP authentication, their login fails with the following error:
  `LDAP: error code 49 - 80090308: LdapErr: DSID-0C0903C5, comment: AcceptSecurityContext error, data 773, v2580]`

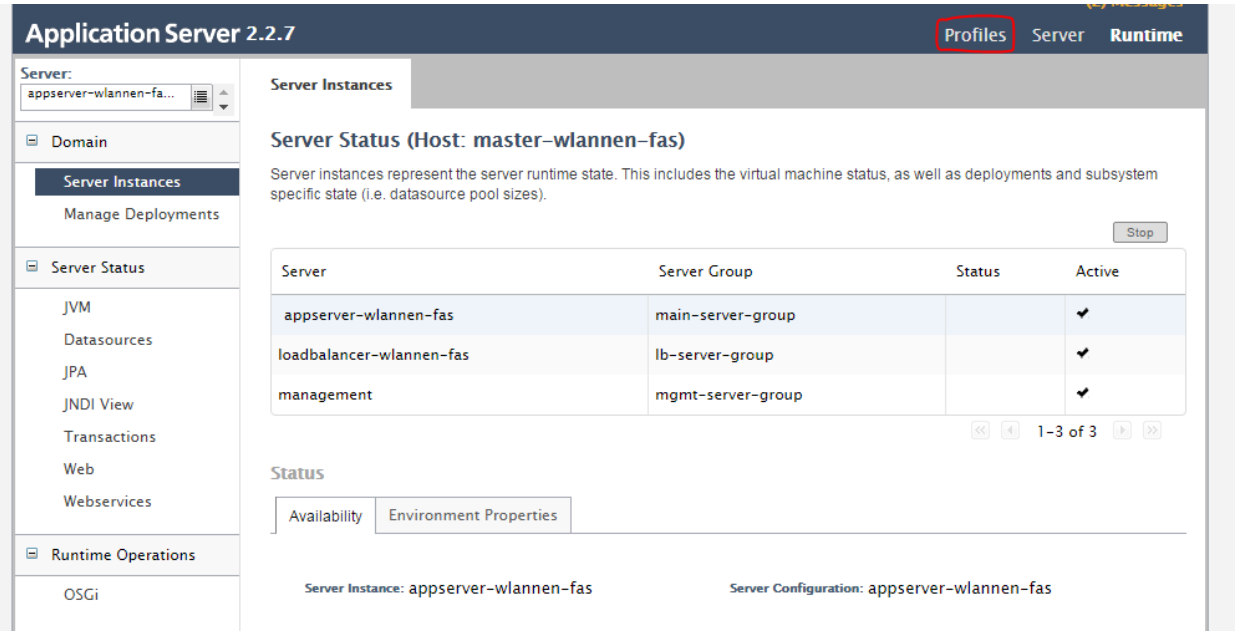
  Workaround:

- Before attempting to use their credentials for LDAP authentication, log the user in using their Active Directory credentials on a system that will prompt to change the password, or
- Do not select the option 'User must change password at next logon' when setting up the user

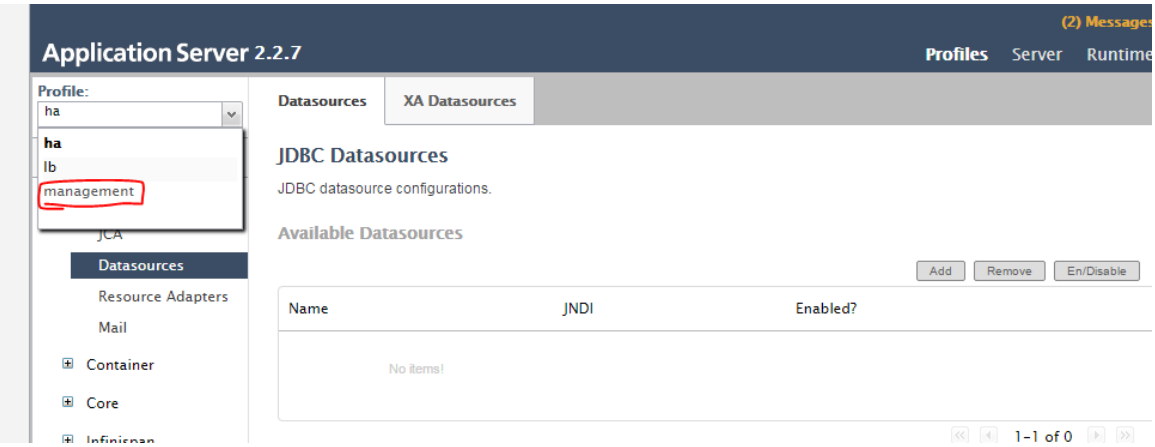
Importing Certificates to the LDAP Trust Store

1. Open the REAS Management Console `https://<Cluster IP or FQDN>:9990`

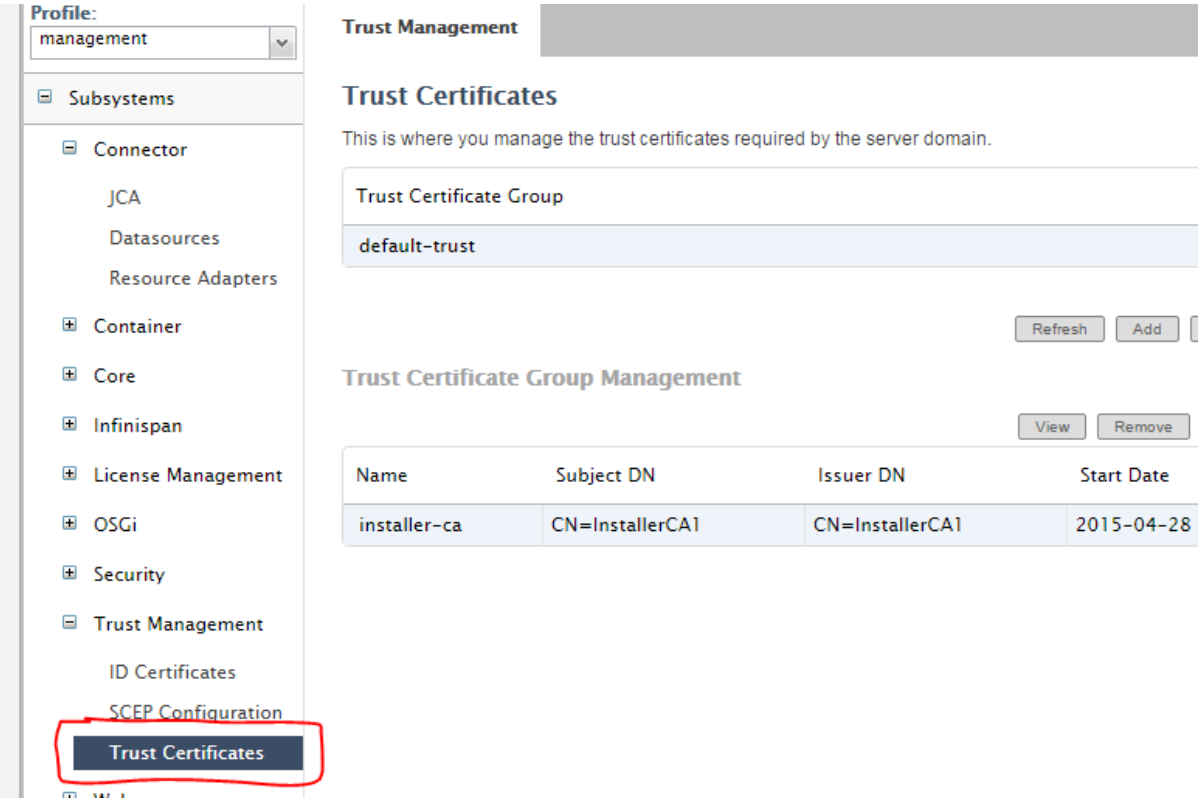
2. Click **Profiles** in the top right.



3. From the Profile drop-down on the left, select management.



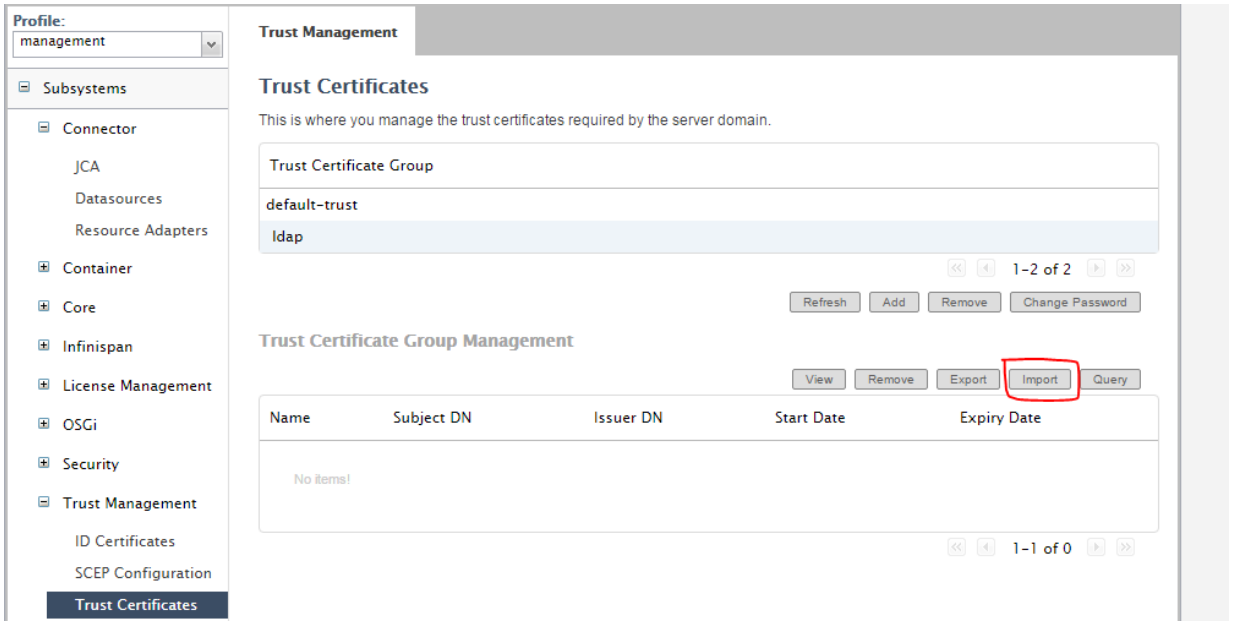
4. In the menu on the right, expand Trust Management, then click Trust Certificates.

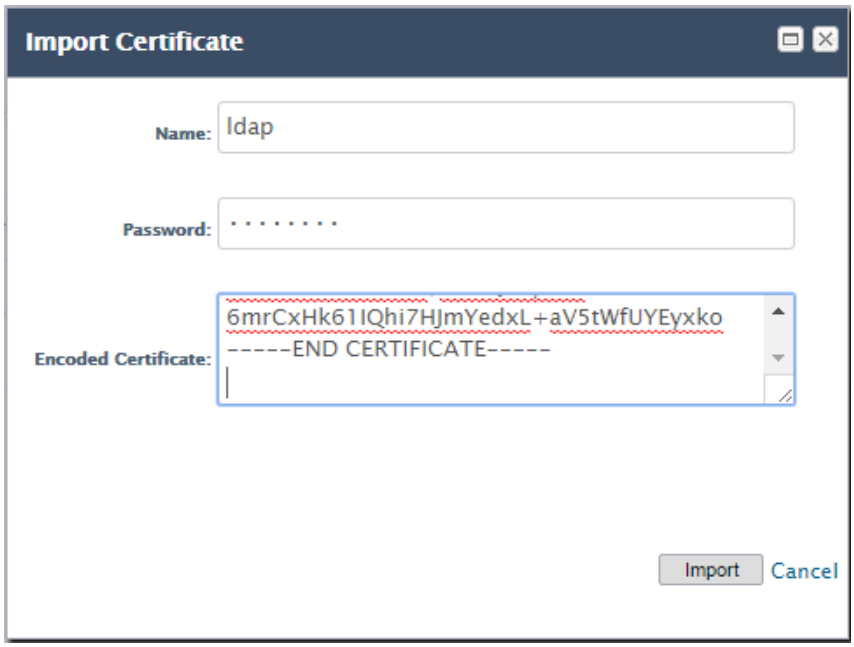


5. On installing CSDK, a trust store called '**ldap**' is created, with the password: `changeit` (this password will be needed when adding certificates or otherwise changing the trust store).

6. Click the row for the '**ldap**' Trust Certificate Group—there should be no certificates listed in the lower table.

7. Click the Import button to add the certificate to the newly added Trust Certificate Group. Enter a name of your choice for the certificate, the password for the trust store (as chosen in step 5), and in the **Encoded Certificate** box paste the contents of the LDAP certificate PEM file (including the `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` lines).



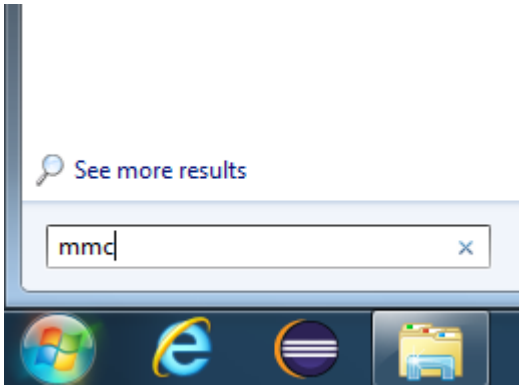


Note: The entire certificate chain for the LDAP server must be fulfilled within the Trust Certificate Group (the main Java truststore is not referenced). In cases where this involves multiple certificates, it will be necessary to repeat step 7 accordingly. See the section Exporting and Converting Certificates from the Windows MMC on page 78 for a possible mechanism to obtain the LDAP server certificate in a Windows environment.

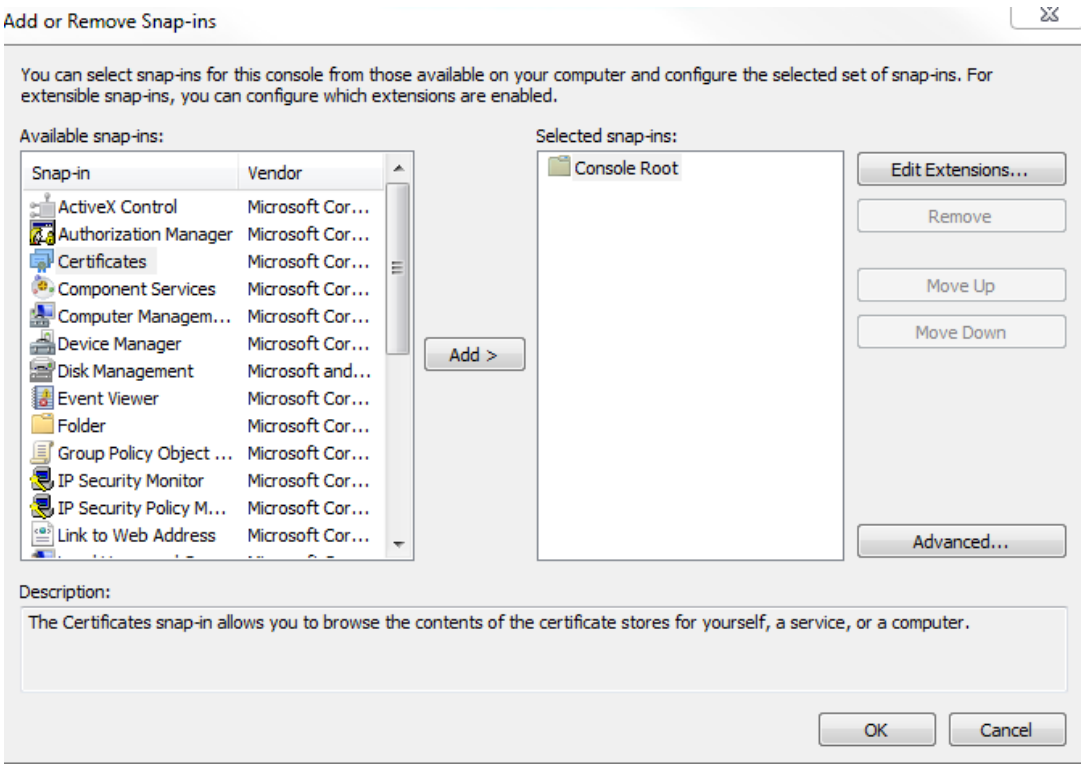
Exporting and Converting Certificates from the Windows MMC

In the case of a Windows environment, the certificate(s) needed to access the LDAP server may be available within the MMC (Microsoft Management Console). For example, if the LDAP server is using a root certificate that is pushed out to users of the same domain, then a user logged into that domain sees this certificate in the MMC.

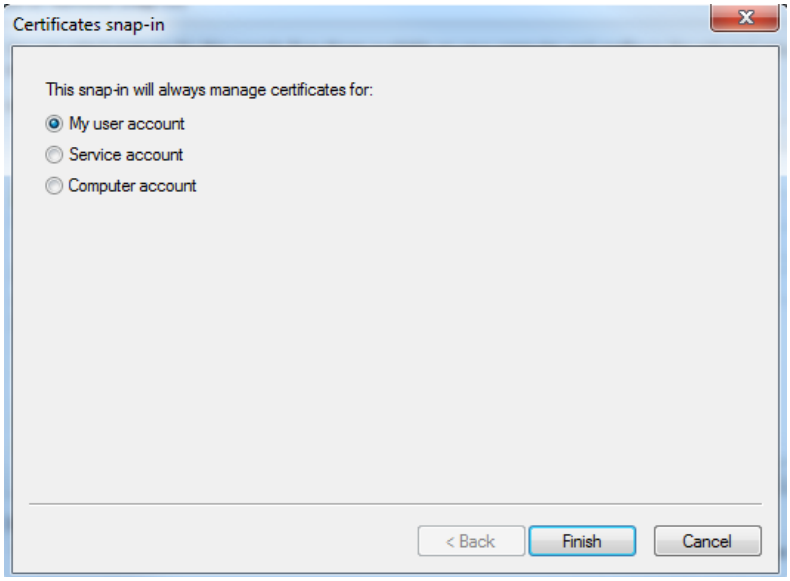
1. Open the MMC in Windows by **Start** > type "**mmc**" > **Enter**.



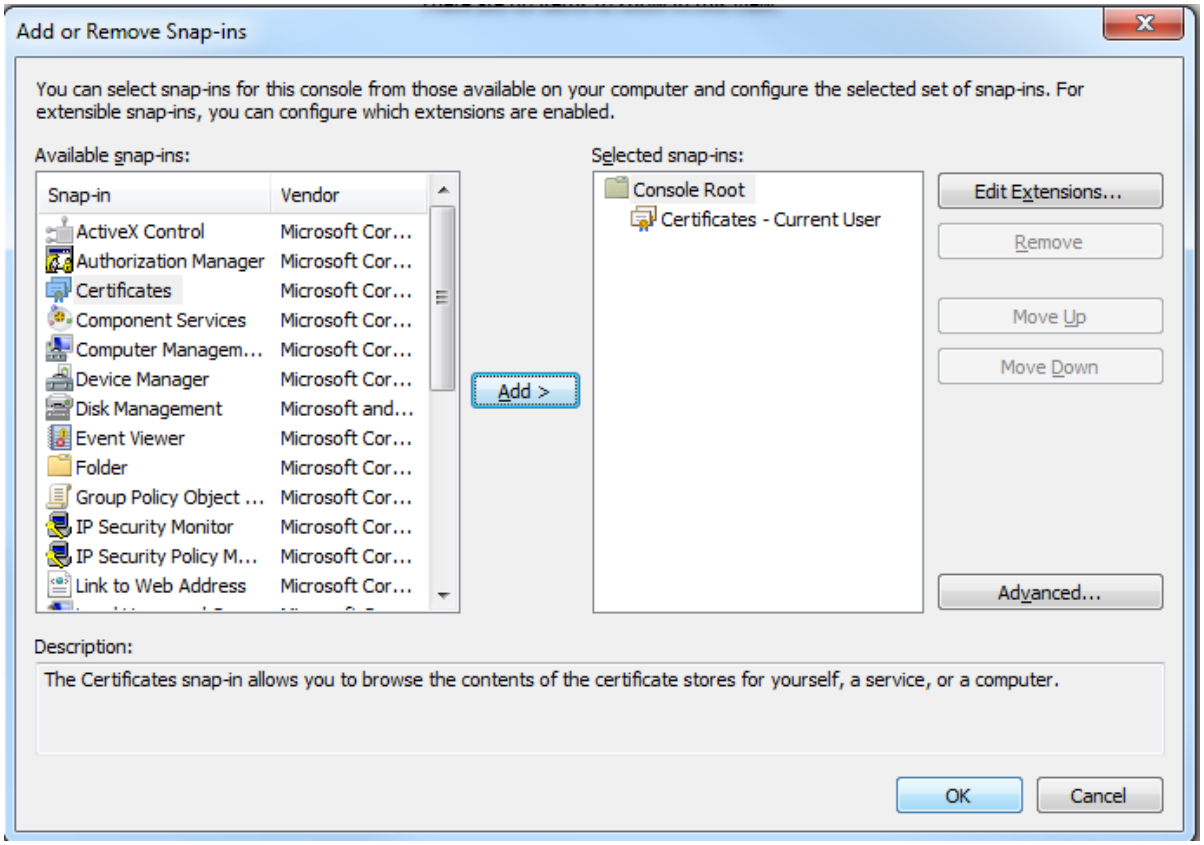
2. Within the MMC, select **File > Add/Remove Snap-in**. Select the Certificates snap-in on the left, then click **Add**.



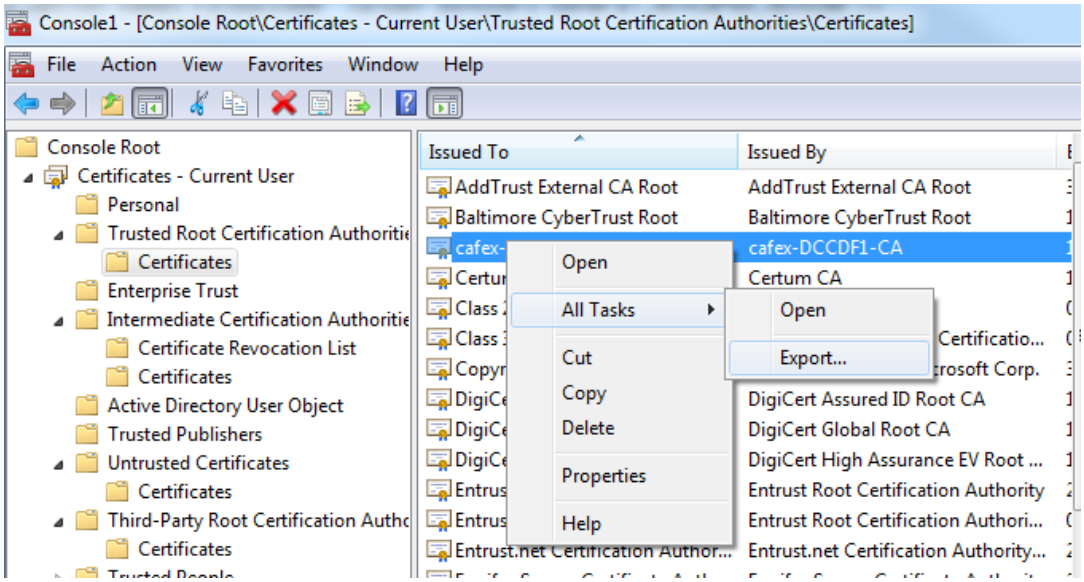
3. When prompted confirm that the snap-in will manage certificates for the user account.



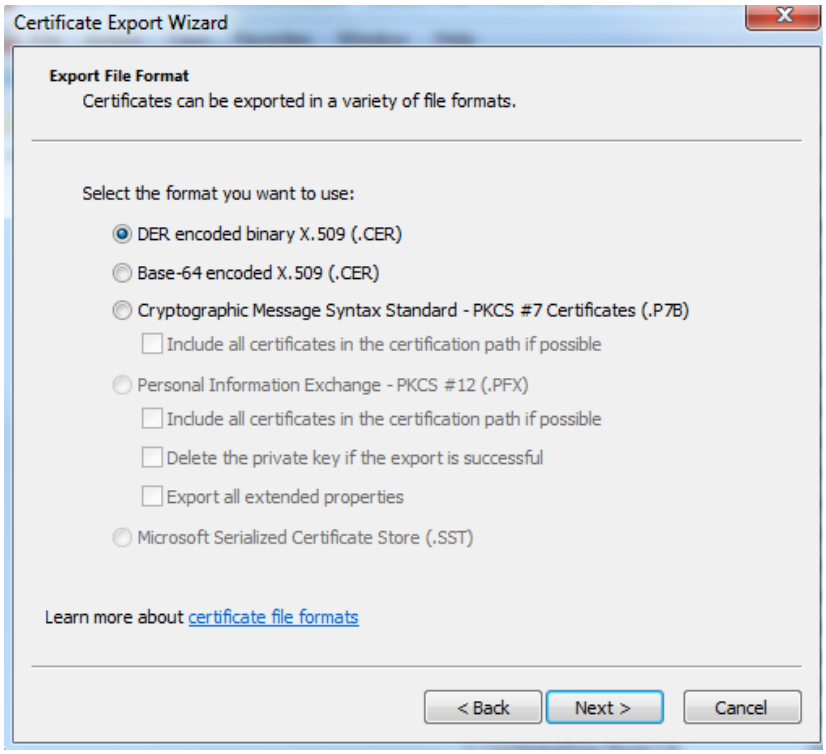
4. Click **OK** to add the snap-in.



5. Expand the tree on the left, locate the required certificate, then click it and select **All Tasks > Export**.



6. When prompted by the wizard, select DER as the format, then save the file to a suitable location.



7. The file can then be converted to **PEM** format using **openssl**, as follows:

```
openssl x509 -inform der -in in_certificate.cer -out out_certificate.pem
```

Note: OpenSSL is typically available at the command line on a Linux-based system; binaries for Windows are also available—see https://www.openssl.org/community/binaries.html

Configuring IE and Safari Plug-Ins

To configure the plug-ins that this release of RE Mobile is compatible with, use the following procedure:

1. Log into the RE Mobile Web Administration Console
   `https://<Cluster IP or FQDN>:8443/web_plugin_framework/webcontroller`
   using the credentials you configured when you ran the **setup.sh** script

2. Under **General Administration > Browser Plugin Management**, for IE and Safari enter the following:

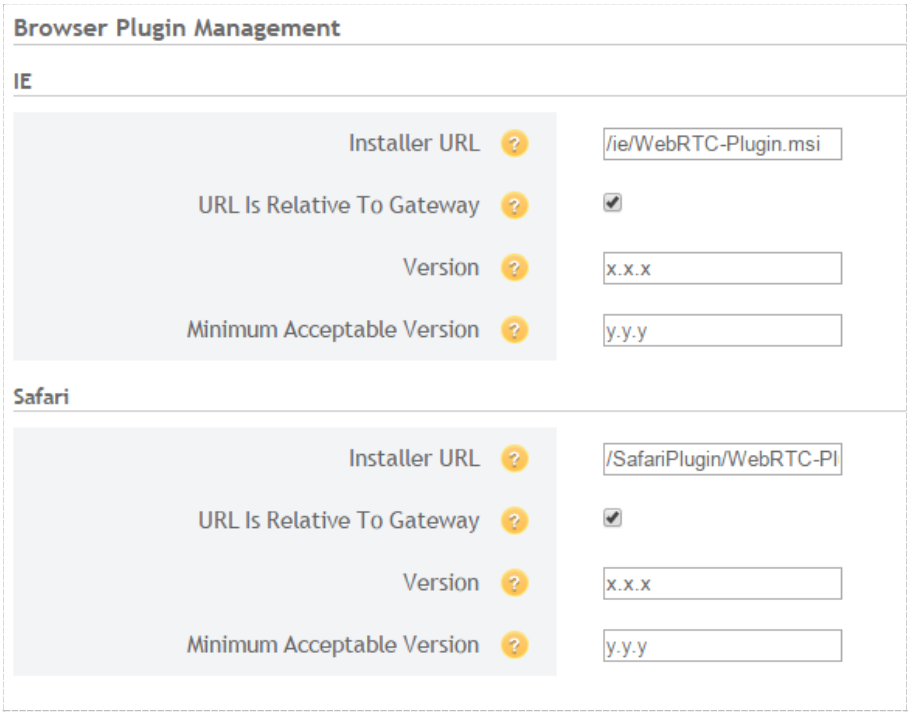
   a. The **Installer URL**—this is normally inserted for you, but you can change the URL, if required.

   b. **URL is Relative to Gateway** checkbox—this is normally checked, meaning that the installer is on the same box as the Gateway, at a relative URL

   c. The current **Version** number of the plug-in installed by the installer at the specified URL—this is available in the *Cisco Remote Expert Mobile—Release Notes*.
   This should normally be set to the current version of the plug-in—if a customer has a plug-in installed that is less than this version, they will be offered to install the new version, but if they already have the Minimum Acceptable Version they will be able to access the service without upgrading.

   The plug-in **Minimum Acceptable Version** number that a user can use—this is available in the *Cisco Remote Expert Mobile—Release Notes*.
   This must be set to at least the earliest compatible version for your software. We recommend that you set this to the current version where possible, in order to provide the best service—this means that any customer attempting to use the service with an older version is required to download and install the new version of the plug-in to access the service.

   Note: When you upgrade or install a new version of Remote Expert Mobile, you may need to update the **Version** and the **Minimum Acceptable Version**. New installations default to the last compatible version. When you want to offer your customers the new plug-in version, you should update these versions appropriately. If the plug-in is hosted on a separate server, you must update the version numbers after you are sure that the correct version of the plug-in is uploaded to that server, and ensure that the **Installer URL** is set to the correct URL.



3. Click **Save**.

Configuring SNMP

Configuring SNMP Trap Targets

To add an address for receiving traps, add an SNMP trap target using the Jboss CLI. The CLI is at the following location:

```
<reas-install-dir/bin/jboss-cli.sh
```

Run the `jboss-cli.sh` command and connect to the Application Server that you have configured as master by running the following command:

```
connect <machine_name>
```

To add the SNMP trap target, use a command in the following format:

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

Where the following apply:

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

For example, to add a target with an ID of '`local`', use a command similar to the following:

```
/profile=management/subsystem=snmp_subsystem/traptarget=local/:add(protocol=SNMPv2c,ip=127.0.0
.1,port=1062)
```

The properties for each trap target can be changed using a command that specifies the `target-name`, for example, to change the port for the '`local`' trap target to `1063`, you would use a command of the following format:

```
/profile=management/subsystem=snmp_subsystem/trap-target=local/:writeattribute(name=port,value=1063)
```

If any changes are made to the SNMP trap target options, the SNMP service must be restarted. This can be done using the following command:

```
/profile=management/subsystem=snmp_subsystem/:restart-snmp
```

Configuring the SNMP client

We recommend that you use an SNMP client that implements the `ALARM-MIB` file—you can download this file from a site such as http://www.simpleweb.org/ietf/mibs/. Import this file into your SNMP client tool, along with any MIB files supplied with applications that will be deployed and raising traps.

For the REAS traps, you import the following MIB files into your SNMP client, in the order shown:

1. `AS-COMMON.MIB`
2. `AS-PLATFORM.MIB`

These files are located in the `<reas-install-dir>/doc/mibs` directory.

REAS SNMP traps

There are a number of SNMP traps that might be raised when significant events occur within the cluster. The following SNMP traps for the RAS are symmetric—this means that each trap contains '`Set`' when an issue is detected, or '`Clear`' when the issue is resolved.

The `Set` traps are as follows:

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

When the issue is resolved, the associated `Clear` trap is raised, for example, if the `platformSetServerGroupDown` trap is raised and at least one server in the cluster is started, the `platformClearServerGroupDown` trap is raised, signifying that the issue is resolved. There is also an asymmetric trap, `platformAbnormalServerShutdown`—this trap is raised every time a REAS shuts down unexpectedly. By default, when an unexpected shutdown is detected, the Host Controlled restarts that server. This trap ensures that administrators are alerted to multiple restarts that might affect service, so that they can investigate the issue

How to decode the resource ID

The resource ID can be thought of as the index into a database table (SNMP table), or an OID identifying a scalar value. The resource ID is made up of an OID and an optional index. The first element is the OID identifying the table or scalar value; if the OID is a table, there is a second element, which is the key defined for that table.

- All the table and scalar OIDs for the REAS trap resources start with `1.3.6.1.4.1.7377.100`
- The scalar Host Controller name has the extension `.0` (an OID of `1.3.6.1.4.1.7377.100.0`)
- The server table has the extension `.1` (an OID of `1.3.6.1.4.1.7377.100.1`)
- The Server Group table has the extension `.2` (an OID of `1.3.6.1.4.1.7377.100.2`)

For the tables, the keys are encoded strings containing the server name for the server table, or the Server Group name for the Server Group table. The encoded string that makes up the index is made up of a number representing the number of characters for the string, followed by the ASCII character numbers that make up the string.

For example, for a server named ‘Hello’, the resource OID would be:

```
1.3.6.1.4.1.7377.100.1.5.72.101.108.108.111;
```

Where the following apply:

- `1.3.6.1.4.1.7377.100.1` is server table OID
- `5` is the length of the string
- `72`—ASCII **H**
- `101`—ASCII **e**
- `108`—ASCII **l**
- `108`—ASCII **l**
- `111`—ASCII **o**

Traps raised on REAS start-up

When a REAS cluster is first started, a number of traps are raised; this is because the system has no history of traps raised, so the status of each server is tested. If the status is fine, a `Clear` trap is raised, regardless of any previous state. Therefore, on start-up it is expected that at least the `platformClearNodesNotRegisteredWithLoadbalancer` and `platformClearServerGroupDown` traps are raised.

As the servers in a REAS cluster are started in an undefined order, it is likely that some `Set` traps are raised, closely followed by the associated `Clear` traps.

Additional Information

Supported features

- **SAN with Fibre interconnect** - Use of a SAN with Fibre interconnect, rather than a NAS, is recommended in order to maximize the transfer speed.
- Incremental VMware Backups - If incremental backups are to be enabled, ensure that you follow the VMware Guides on 1st and 3rd Party Backup Solutions.

Unsupported features

- **VMware fault tolerant mode** - VMware fault tolerant mode is not supported (because the Remote Expert Mobile uses multiple cores).
- **vMotion** - vMotion has not been tested with Remote Expert Mobile.

  Note: VMware snapshots are not supported, and will cause performance issues

Customer ANI is not passed to agent2

See also the *Release Notes* > *Limitations and Restrictions* section for further details on this issue.

- Symptoms
  - When a consult transfer is initiated from agent1 to agent2 with ViQ, the customer ANI is not passed to agent2
- Scenario
  1. Install RE Mobile application and create a PCCE environment for solution testing of RE Mobile.
  2. Initiate a customer call from any browser.
  3. Login an agent1 using Expert Assist gadget (Finesse) and make them available.
  4. Answer the call from agent1 side and initiate a consult call (with ViQ being played).
  5. Login an agent2 using Expert Assist gadget (Finesse) and make them available.
  6. Answer the call from agent2 side and complete the transfer from agent1 side.
  7. Now the call is established between the customer and agent2.
     Once the transfer is complete, agent2 should get customer ANI on agent phone and Finesse desktop—however agent2 is not getting the customer ANI on Finesse desktop, but is getting the customer ANI on agent phone.
     (After step4 without ViQ the above scenario works without any problems.)
- Workaround
  1. Set the ANI of the customer to a Peripheral variable say PV1 in the initial script where the call is sent to Agent 1.
     `Call.peripheralvariable3=Call.CallingLineID`
  2. In the transfer script when the agent initiates the transfer, set
     `Call.CallingLineID = call.Peripheralvariable3`

Upgrade and Rollback

This section describes the process for upgrading an existing Remote Expert Mobile installation or rolling back to a previous version.

Note:

- Upgrading RE Mobile affects the service; the RE Mobile cluster will be unavailable whilst the upgrade is taking place.
- With version 11.5(1), the upgrade process has changed significantly—it is not possible to roll back to an earlier version than this after running the revised upgrade procedure.

Upgrade Procedure

We support upgrading to the latest version of 11.5(1) from the latest version of the following releases:

- 10.6(2)
- 10.6(3)

See Checking the RE Mobile Version on page 90.

If you are not using the latest version of one of the above releases, see Upgrading from Older Versions on page 88, and then use this upgrade procedure to bring your installation completely up-to-date.

Preparation Stage

Run this preparation stage once only.

1. Expand the OS disk size
   a. Open the VMware Infrastructure (VI) Client and connect to **VirtualCenter** or the **ESXi host**
   b. Right-click on the virtual machine
   c. Click **Edit settings**, and select the virtual disk
   d. In the box on the right, increase the HDD size to at least **48 GB**
   Note: A VMWare restriction prevents you from expanding a virtual disk for which a snapshot has been taken.
2. Reboot the VM
3. Download the `rem-<version>-os-prepare.tar.gz` archive into the `/tmp` directory.
4. Change to the `/tmp` directory
   `cd /tmp`
5. Extract the archive—run
   `tar -xf REM-<version>-os-prepare.tar.gz`
6. Run
   `./os-prepare.sh`
   After about 5 minutes, the following message will display: “System has been successfully prepared.”

Upgrade Stage

Note: There is no need to stop any services before running the upgrade process.

Perform the upgrade on the servers in the following order:

1. REAS Master
2. Slave Nodes
3. REMB Nodes

1. Download the `rem-<version>-full-upgrade.upf` upgrade file into the `/tmp` directory.

2. Change to the `/tmp` directory:
   `cd /tmp`

3. Run:
   `/opt/cisco/bin/full-upgrade.sh -f REM-<version>-full-upgrade.upf`

   Note: For subsequent upgrades, As the REM Admin user (for example, **rem-admin**), run:
   `sudo /opt/cisco/bin/full-upgrade.sh -f REM-<version>-full-upgrade.upf`

4. Follow the prompts as detailed below, when asked for the usernames and passwords for the installed system (the on-screen text is shown in italics below)

   a. If you are upgrading from version 10.6, you will be prompted for the following new and old users, as explained below:

      i. Admin credentials:
      The version you are upgrading to has a new authentication system. The <admin> credentials are now used for authenticating user access to both the REM Web Admin Console and the REAS Management Console. These need not match any credentials used in the system you are upgrading from.

      ii. Master/Slave credentials:
      The version you are upgrading to has a new authentication system. The new <master/slave> credentials are used for authenticating access to the master node from any slave nodes (i.e. this is not for user access). These are new and do not match any credentials used in the system you are upgrading from. The same master/slave credentials need to be used across all REAS nodes in the cluster. Please note that the username and password cannot be equal to each other.

      iii. Old administrator:
      As you are upgrading from a system which has an old authentication system, the <old administrator> credentials used in that system are now required.

      iv. New users—the default usernames are shown below, but set the usernames and passwords to whatever you want for the different levels of security (see REM Users and Security on page 11):
      rem-user
      rem-admin
      rem-ssh

   b. If you are upgrading from version 11.x, you will be prompted for the following existing users—use the same usernames and passwords that you set when running `setup.sh`.

      i. Admin credentials
      The <admin> credentials are used for authenticating user access to both the REM Web Admin Console and the Management Console. These must match the <admin> credentials used in the system you are upgrading from.

      ii. Master/Slave credentials
      The new <master/slave> credentials are used for authenticating access to the master node from any slave nodes (i.e. this is not for user access). These need not match any credentials used in the system you are upgrading from. The same master/slave credentials need to be used across all

REAS nodes in the cluster. Please note that the username and password cannot be equal to each other.

iii. Users—the default usernames are shown below, but use the usernames and passwords you set when you ran the `setup.sh` script (see REM Users and Security on page 11):
rem-user
rem-admin
rem-ssh

5. Wait for the upgrade to proceed.
The machine will reboot several times, and the upgrade should take about 30 minutes.
Note: The upgrade process writes the following log: `/var/log/app-upgrade.log`

Upgrading from Older Versions

Important: It is possible to upgrade from release 10.6(1) to the latest version of the following releases using the procedure in this section:

- 10.6(2)
- 10.6(3)

See Checking the RE Mobile Version on page 90.

Having upgraded to latest version of one of the above releases, to complete the upgrade to the latest version of 11.5(1), use the additional procedure described in Upgrade Procedure on page 86.

The upgrade procedure typically takes 20 minutes for each REAS master node and 5 minutes for either a REAS slave node or REMB node.

Your installation may be made up of any of the following:

- A single node running both a master REAS and REMB
- Two nodes, one running a master REAS and one running REMB
- Four nodes, one master REAS, one slave REAS and two running REMB

In all these cases the procedure is as follows:

1. Stop the REAS and REMB services on all nodes.

   See Stopping Services below.

2. Run the upgrade script on each of the nodes in the following order:

   a. REAS Master

   b. REAS Slave

   c. REMB—update each in turn in any order

   See Upgrading a Node on page 89.

Stopping Services

For nodes running REAS, run:

```
service reas stop
```

For nodes running REMB, run:

```
service media_broker stop
```

This command stops the Media Broker immediately. You may prefer to shut down the Media Broker gracefully using the following command; this prevents new calls from starting, but allows existing calls to continue.

```
service media_broker request shutdown
```

For nodes running both services you must run both commands.

Upgrading a Node

To upgrade a node, follow these steps:

1. Copy the upgrade package (for example, `REM-upgrade-11.5.1.10000-n.tar.gz`) to the node's tmp directory.

   ```
   scp REM-upgrade-*.tar.gz root@reas-node:/tmp
   ```

2. Run the upgrade script against the upgrade package

   ```
   /opt/cisco/bin/upgrade.sh -f /tmp/REM-upgrade-<version>.tar.gz
   ```

3. The upgrade script will take you through the following steps

   a. Confirm upgrade

   b. Accept license terms.

   c. For Master REAS nodes the following additional steps are included

      1. Enter REAS administrator username/password: (default is administrator/administrator)

      2. Enter REAS REST username/password (default is administrator/administrator)

   d. Confirm shutdown of service(s)

      Note: this step will print `FAILED` if the services have already been stopped, the message can be safely ignored.

4. The installation will complete and the REAS and/or REMB service(s) will be automatically restarted.

5. Repeat these steps for each node in the RE Mobile cluster

After RE Mobile is upgraded the RE Expert Assist Agent and Supervisor Finesse gadgets may be cached by Finesse for 60mins. The cache can be cleared by restarting the Cisco Tomcat process on the Finesse Server, restarting Cisco Tomcat is described in the *Cisco Finesse—Administration Guide*.

After a successful upgrade, the directory structure will look like the following (although the version numbers may differ on your install):

```
/opt/cisco
+--- 10.6.1.10000-8
|         +---BIN
|         +---CSDK
|         +---REAS
 +--- 10.6.2.10000-2
|         +---BIN
|         +---CSDK
|         +---REAS
+--- bin->10.6.2.10000-2/BIN
```

Important: Having complete the upgrade to this version, now upgrade to the latest version using the additional procedure described in Upgrade Procedure on page 86.

Upgrade from Remote Expert Co-browse to Expert Assist

Upgrading from Remote Expert Co-browse to REM Expert Assist is not directly supported. To do so, install new REMB nodes as on page 23, and add them to the existing master REAS node.

Roll back to a previous version

All nodes in the cluster must be rolled back to the same versions. The rollback procedure for a cluster is:

1. Stop the REAS and REMB services on all nodes.

   See “Stopping Services” above.

2. Roll back the nodes (see Rolling back a node below) in the following order:

   a. REAS Master

   b. REAS Slave

   c. REMB—roll back each in turn, in any order

Rolling back a node

To roll back a node to a previous version of RE Mobile, following a full upgrade, reinstate the inactive OS that you upgraded from:

1. To list the current active and inactive OSs, use:

   ```
   /opt/cisco/bin/os-list.sh
   ```

2. To switch to the inactive OS that you upgraded from, use:

   ```
   /opt/cisco/bin/os-switch.sh
   ```

Checking the RE Mobile Version

To check which version of RE Mobile a cluster is running, perform the following steps

1. Log into the RE Mobile Web Administration Console
   `https://<Cluster IP or FQDN>:8443/web_plugin_framework/webcontroller`
   using the credentials you configured when you ran the **setup.sh** script.

2. The page will display the RE Mobile version number, for example.

   — Gateway Administration Portal (Product Version: **11.5.1.10000-21**)

Acronym List

Item	Description
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-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
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