THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

© 2015 Cisco Systems, Inc. All rights reserved.
Preface

Change History

<table>
<thead>
<tr>
<th>Changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>First published</td>
<td>2015-07-31</td>
</tr>
<tr>
<td>Added section on Upgrade</td>
<td>2015-08-20</td>
</tr>
</tbody>
</table>

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 & 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 10.6”.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
## Organization of This Guide

This guide includes the following sections:

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introduction</strong></td>
<td>Introduction &amp; brief overview of Remote Expert Mobile and its SDKs, software server components, agent integrations and key technologies.</td>
</tr>
<tr>
<td><strong>Overview of Remote Expert Mobile Deployment Options</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Before You Begin</strong></td>
<td>Lists Infrastructure requirements.</td>
</tr>
<tr>
<td><strong>Installing RE Mobile for a Single Master Node / All-In-One Deployment</strong></td>
<td>Table showing sequence of operations required to install RE Mobile for a single node deployment.</td>
</tr>
<tr>
<td><strong>Installing the Base Multi-node HA Deployment</strong></td>
<td>Table showing sequence of operations required to install RE Mobile for a single node deployment.</td>
</tr>
<tr>
<td><strong>Install and Configure the Virtual Machine(s)</strong></td>
<td>Describes hardware, software and configuration requirements for the virtual machine(s) needed to run RE Mobile.</td>
</tr>
<tr>
<td><strong>Configure the NTP Service</strong></td>
<td>Describes the procedure for configuring the NTP service.</td>
</tr>
<tr>
<td><strong>Configure the HTTP Reverse Proxy</strong></td>
<td>Describes the configuration of the reverse proxy needed for RE Mobile.</td>
</tr>
<tr>
<td><strong>Configure the Domain Name Service (DNS)</strong></td>
<td>Describes the procedure for configuring the DNS service.</td>
</tr>
<tr>
<td><strong>Install the Remote Expert Mobile OVA</strong></td>
<td>Describes the procedure for installing the REM OVA. Includes subsections for Single- and Multi-node deployments.</td>
</tr>
<tr>
<td><strong>Configuration and use of Transport Layer Security (TLS) in REAS</strong></td>
<td>Ensure successful installation of TLS certificates.</td>
</tr>
<tr>
<td><strong>Operating System</strong></td>
<td>Describes how to gain access to the hosts’ operating systems.</td>
</tr>
<tr>
<td><strong>Remote Expert Mobile Administration Console</strong></td>
<td>Describes how to access the REM Administration Console.</td>
</tr>
<tr>
<td><strong>Expert Assist Configuration – Consumer Access Number Regex</strong></td>
<td>Configuration of destination number restriction by regular expression.</td>
</tr>
<tr>
<td><strong>Expert Assist Configuration – Image Quality Scale Factor</strong></td>
<td>Configuration of screen share quality using Expert Assist.</td>
</tr>
<tr>
<td><strong>Post Install Verification</strong></td>
<td>Perform test calls and Expert Assist sessions.</td>
</tr>
<tr>
<td><strong>Integrating Remote Expert Mobile</strong></td>
<td>Ensure successful RE Mobile integration with your UC or CC environment.</td>
</tr>
<tr>
<td><strong>Restricting Application URIs via the Reverse Proxy</strong></td>
<td>List of the URIs that should be allowed through the Reverse Proxy.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold font</strong></td>
<td>Commands and keywords and user-entered text appear in <strong>bold font</strong>.</td>
</tr>
<tr>
<td><em>italic font</em></td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <em>italic font</em>.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td><strong>courier font</strong></td>
<td>Terminal sessions and information the system displays appear in <strong>courier font</strong>.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>
Introduction

Cisco Remote Expert Mobile is a software solution that enables personal and actionable customer interactions within mobile & web applications. These interactions range from simple click-to-call to a complete voice, video and Expert Assist customer engagement session interconnected to a full contact center environment. For example, Cisco Remote Expert Mobile can connect individual investors to the next available financial advisor within a mobile trading app (B2C – Business to Consumer) or a field employee’s mobile app routing into an internal helpdesk (B2E – Business to Employee).

Features

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

- **In-app voice & video communications (Over-the-Top WebRTC communications)**
  - High definition video and audio
  - Bi-directional or one-way video
  - Mute audio, video or both
  - Client side call control
- **WebRTC to SIP gateway (trunking into Cisco Unified Border Element and Unified Communications Manager)**
- **Expert Assist**
  - Web co-browse
  - Mobile app sharing
  - Remote app control
  - Expert form editing and completion
  - Annotation by expert
  - Expert document push
  - Expert URL sharing
  - Protect sensitive data with field and data masking
- **Media Handling:**
  - STUN server (RFC 5389) for client external IP identification
  - UDP port multiplexing
  - Media encryption / decryption
  - Bidirectional audio
  - High definition video (H.264 or VP8 in CIF (352x288), nHD (640x360), VGA (640x480), 720p (1280x720)
  - High definition and narrowband audio codec support (Opus, G.711 ulaw or G.711 alaw)
  - Opus, G.711 ulaw, G.711 alaw & G.729a audio transcoding into the enterprise network
  - H.264 & VP8 video transcoding

SDKs

Cisco Remote Expert Mobile includes Software Development Kits (SDKs) to provide voice over IP, video over IP and expert assist (app share & web co-browse, annotation and document push) features within pre-existing mobile and web applications. Whether placing or receiving calls in
client web applications, RE Mobile’s Client SDK for Web supports every major browser such as: Google Chrome 33+, Mozilla Firefox 28+, Opera 28+, Internet Explorer 11 and Apple Safari 6+. With WebRTC at its core, in-app communications are enabled without the need for plugins. Where WebRTC is yet to be supported in Internet Explorer and Safari, WebRTC plugins are provided for voice and video. Cisco Remote Expert Mobile also delivers integrated communications in iOS 7+ and Android 4.1.2+ apps thru native libraries.
Overview of Expert Mobile Deployment Options

As detailed in Remote Expert Mobile Design Guide 10.6, 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 (Application Server and Media Broker) 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: It is important to note that the OVA will **ALWAYS** create a VM hosting both the REAS (which hosts the Web Gateway, Expert Assist as well as the Finesse Gadgets and Expert Assist Web Consoles) and 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 and CUCM. This guide does not cover Remote Expert Mobile deployed exclusively with Unified CM.

**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.
Figure 1. Single Node Topology

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.

Multi-node, Clustered Topology

Remote Expert Mobile Base HA Multi-node Deployment is a four (4) node cluster (2 REAS and 2 REMB) and can support up to 100 concurrent video, audio and expert sessions in a high availability configuration.
Figure 2. Base HA Multi-node Deployment

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

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

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-on-one deployment are shown in the table below:

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Done?</th>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>Install and configure the virtual host</td>
<td>Install and Configure the Virtual Host(s)</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Configure NTP</td>
<td>Configure the NTP Service</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Install and configure the HTTP Reverse Proxy</td>
<td>Configure the HTTP Reverse Proxy</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Install and configure DNS</td>
<td>Configure the Domain Name Service (DNS)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Deploy the OVA for Single Master Node / All-In-One deployment</td>
<td>Installing a Single Master Node / All-In-One Deployment</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Verify the installation.</td>
<td>Post Install Verification</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Configure Transport Layer Security in REAS</td>
<td>Configuration and use of Transport Layer Security (TLS) in REAS</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Log into the host’s operating system</td>
<td>Operating System</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Use a browser to access the Remote Mobile Administration Console</td>
<td>Remote Expert Mobile Administration Console</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Configure Remote Expert Assist</td>
<td>Expert Assist Configuration – Consumer Access Number Regex</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Integrating RE Mobile into a Contact Center Environment</td>
<td>Integrating RE Mobile into a Contact Center Environment</td>
<td></td>
</tr>
</tbody>
</table>

Error! Reference source not found.
### 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:

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Done?</th>
<th>Task</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>Install and configure the virtual host</td>
<td>Install and Configure the Virtual Host(s)</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>Configure NTP</td>
<td>Configure the NTP Service</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Install and configure the HTTP Reverse Proxy</td>
<td>Configure the HTTP Reverse Proxy</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Install and configure DNS</td>
<td>Configure the Domain Name Service (DNS)</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Deploy the OVA for Base Multi-node HA deployment</td>
<td>Installing a Base Multi-node HA Deployment</td>
</tr>
</tbody>
</table>

<p>| 12       |       | Test the Agent Console                                              | Testing the CC Integration                     |
| 13       |       | Restrict Application Via the Reverse Proxy                          | Restricting Application URIs via the Reverse Proxy |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Install and Configure the REMB for Base Multinode HA deployment</td>
<td>Installing and Configuring a REMB (Base Multi-node HA deployment)</td>
</tr>
<tr>
<td>7</td>
<td>Verify the installation</td>
<td>Post Install Verification</td>
</tr>
<tr>
<td>8</td>
<td>Configure the Transport Layer Security (TLS) in REAS</td>
<td>Configuration and use of Transport Layer Security (TLS) in REAS</td>
</tr>
<tr>
<td>9</td>
<td>Log into the host’s operating system</td>
<td>Operating System</td>
</tr>
<tr>
<td>10</td>
<td>Use a browser to access the Remote Mobile Administration Console</td>
<td>Remote Expert Mobile Administration Console</td>
</tr>
<tr>
<td>11</td>
<td>Configure Remote Expert Assist</td>
<td>Expert Assist Configuration – Consumer Access Number Regex</td>
</tr>
<tr>
<td>12</td>
<td>Integrating RE Mobile into a contact center environment</td>
<td>Error! Reference source not found.</td>
</tr>
</tbody>
</table>
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 RE Mobile. The minimum requirements for future releases may differ and you should refer to the release notes or administrator guide to ensure that pre-requisites are met.

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](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**

1. **Step 1** Select the host.
2. **Step 2** Go to the Configuration tab.
3. **Step 3** Select Time configuration.
4. **Step 4** Select Properties.
5. **Step 5** If the date and time were red on the previous page, set the date and time manually to the current time.
6. **Step 6** Click Options.
7. **Step 7** Select NTP Settings and click Add.
8. **Step 8** Enter the IP address of the NTP server and click OK.
9. **Step 9** Select Restart NTP service to apply changes check box
10. **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 Apache, F5, and Nginx.

For information on configuring HTTP Reverse Proxy, see the documentation for the specific Reverse Proxie that you’re 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 will outline installation for the two 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 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, please be sure to review the Cisco Remote Expert Mobile 10.6 Design Guide.

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

The steps below describe how to deploy the simplest RE Mobile configuration.

*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.

Note: You may change the default template name to something more descriptive if you wish.

Step 9: Select the desired hardware deployment configuration.

The deployment template enables you to choose from one of two VM hardware configurations – Small Machine or Large Machine.

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


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

b. Remote Expert Mobile – Large Machine

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

Select Remote Expert Mobile – Small Machine, 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.

18
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 a single node deployment, the only interface required is the “External”. As the others will not be enabled, their associations are irrelevant.

**Step 13:** Configure the template network details.

a. **Node Configuration**
   
   I. **Node Type** - For a single node deployment, there will only be one Application Server, therefore, the Node Type must be set to **Master**.
   
   II. **Cluster Address** - For a single node deployment, use the (DNS-resolvable) FQDN of the host.
   
   III. **Master Node Address** - For a single node deployment, this property is irrelevant and should be ignored.

b. **Network Name Resolution**

   I. **Host Name** - Specify the desired hostname of the VM being installed. This should be a DNS-resolvable FQDN.
   
   II. **DNS Server 1** - This is a **mandatory** field. Enter the address of DNS server that the RE Mobile VM should use.
   
   III. **DNS Server 2** - The second DNS server is an optional field.

c. **Network Time Configuration**

   Configuring NTP is highly recommended, and therefore should be enabled with an appropriate NTP server address e.g. time1.google.com

d. **External Network Configuration**

   As mentioned earlier, configuring the external network is mandatory for each RE Mobile cluster node.

   I. **External IP Address** - 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 selected on the previous screen.

   II. **External Network Mask** - Enter the required network mask (e.g. 255.255.255.0) for the LAN associated with the External interface.

   III. **External Gateway** - Enter the IP address of the External interface’s default network gateway.

   Note that this is NOT related to the Web Gateway hosted on the REAS.

e. **Internal Network Configuration**

   The Internal interface is not required for a single node deployment, therefore the **Use Internal Network** checkbox should be left unchecked.

f. **Management Network Configuration**

   The Management interface is not required for a single node deployment, therefore the **Use Management Network** checkbox should be left unchecked.

**Step 14:** Review the summary, check the box to power on the VM once deployment has completed, and click **Finish** to begin deployment. Details shown in the summary will be written to a file as a record of the selected configuration for later reference.
Step 15: OVA installation will now proceed – wait for it to complete.

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 deploying the OVA.

As such, 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 credentials below:

Username: root
Password: changeit

Note: Run the password.sh script and change the administrator password.

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 the Post Install Verification section below.

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, please read the “Cisco Remote Expert Mobile Design Guide 10.6” for better familiarity with Remote Expert Mobile pre-requisites, architecture and software components.

**Note:** The topology below is an example only.

<table>
<thead>
<tr>
<th>Server Type</th>
<th>OVA Size</th>
<th>Type of Node</th>
<th>OVA Configuration Notes</th>
</tr>
</thead>
</table>
| REAS-A      | Small   | Master       | ▪️ Master: 0.0.0.0 (default)  
▪️ 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 |
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). As shown in the diagram below, the REAS cluster is installed and configured within the enterprise’s internal “green” zone, while the REMB has been placed within the DMZ.

The diagram below shows a typical multi-node deployment consisting of two REAS VMs and the REMB VMs for increased resilience and media handling capabilities.

Required REAS 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 via 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 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 on the Media Broker to configure and control it.

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 8. 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. 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.

   **Note:** 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 two VM hardware configurations. The supported configuration is the “small machine,” described below.

Remote Expert Mobile – Small Machine

Requires 4 vCPU (8400 MHz reservation) & 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 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 (REAS): Select the desired Disk Format as 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 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 Application Server VM being deployed, the required interfaces are the “External” and “Management”. 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): Configure the template network details.

Note: A deployment with multiple REAS nodes requires DNS entries to enable a single domain name to resolve to the external IP addresses of the Master and Slave REAS nodes.

a. Node Configuration (REAS)

I. Node Type - When installing the first REAS in the cluster, the Node Type must be set to Master.

Set the Node Type to Slave when installing subsequent Application Server VMs into the same cluster as the Master.

II. Cluster Address - This property defines an address in DNS that resolves to all the REAS nodes within the cluster.

As illustrated above, this is an optional property that is only applicable when deploying the Master node. If left blank, the Master node’s “External” IP address (which is the default value) will be applied.
If this value is to be set, DNS must be configured with it **before** continuing with this deployment ensuring that the DNS entry resolves to only the Master node.

By setting this value, a new self-signed HTTPS identity certificate will be generated (using this value) for the REAS cluster during deployment.

Also, if this value was set when installing the Master node, then while installing any Slave node, DNS must be updated with a new entry for the Slave’s IP address against this Cluster Address.

**Note:** It is important to update DNS after the Slave VM has been installed.

**III. Master Node Address** - This property is only required by REAS Slave nodes to enable them to communicate with the Master. It should therefore only be populated when a Slave REAS VM is being installed. If the Master node has been configured with a management interface, then the address for that interface should be used.

b. **Network Name Resolution (REAS)**
   i. **Host Name** - Specify the desired hostname of the VM being installed. This should be an FQDN.
   ii. **DNS Server 1** - This is a **mandatory** field. Enter the address of DNS server that the RE Mobile VM should use.
   iii. **DNS Server 2** - The second DNS server is an optional field.

c. **Network Time Configuration**

When installing a multi-node cluster, NTP must be configured by selecting the “Use Network Time Server?” checkbox and specifying an appropriate NTP server address e.g. time1.google.com

d. **External Network Configuration (REAS)**

As mentioned earlier, configuring the external network is mandatory for each VM being created.

I. **External IP Address** - 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 selected on the previous screen.

II. **External Network Mask** - Enter the required network mask (e.g. 255.255.255.0) for the LAN associated with the External interface.

III. **External Gateway** - Enter the IP address of the External interface’s default network gateway.

   Note that this is NOT related to the REAS.

e. **Internal Network Configuration (REAS)**

   Use **Internal Network** checkbox should be left unchecked for REAS. The Internal interface is not required for this REAS’s deployment topology. It is specific to the Media Broker.

f. **Management Network Configuration (REAS)**

As described earlier, the “Management” interface is optional but the Application Server VM in this topology will be configured with 2 interfaces - External and Management.

In order to enable and configure the Management interface, the Use Management Network checkbox MUST be checked.

1. **Management IP Address** - Enter the IP address that will be assigned to this VM’s Management interface when installed.
This must be a valid and available IP address within the network associated with the “Management” interface selected on the previous screen.

2. **Management Network Mask** - Enter the required network mask (e.g. 255.255.255.0) for the LAN associated with the Management interface.

3. **Management Gateway IP Address** – This field should be left blank.

Note that this is NOT related to the REAS.

4. **Management Gateway Remote Network (CIDR format)** – This field should be left blank. If the Application Server is expected to communicate with entities on a different network via this interface, the IP address range (encompassing the other entities) on the other network should be entered (in CIDR format) e.g. 10.10.10.0/24. Configuring this field will cause a static route to be added to the VM’s network routing table.

For a deployment such as the one in which this Application Server VM is being installed, its Management interface will only be used to initiate communication with any slave Application Servers. As they will be on the same subnet, this field should be left blank.

**Step 14 (REAS):** Review the summary, check the box to power on the VM once deployment has completed, and click **Finish** to begin deployment.

**Step 15 (REAS):** OVA installation will now proceed – wait for it to complete.

**Step 16 (REAS):** Post install server access.

On first boot of your new VM, the OS and RE Mobile applications will be configured according to the details entered when deploying the OVA. As such, the first boot of the new VM will take longer than a normal boot. Please do not use the VM until the login prompt is displayed on the console as viewed through the vSphere client.

To SSH into the external address of VM, use the credentials below.

**Username:** root

**Password:** changeit

Disable the Media Broker by executing the following command:

```
/opt/cisco/10.6.1.10000-x/CSDK/resources/disable-service.sh
```

**Step 17 (REAS):** Adding an Additional REAS Slave Node

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

However, note that all subsequent VMs must be added as Slave nodes. Step 13 (above) describes the OVA’s configuration screen where this is set.

**Step 18 (REAS):** Set the cluster address

By default, the RE Mobile Application Server’s cluster address will be set to the IP address of the Master node. If the cluster has more than one REAS node, its cluster address should be changed.

This can be performed during deployment, as described in Step 13 (above). If it has already been done, the following procedure is NOT required, but may be followed if the administrator wishes to change the cluster address.

Before changing the cluster address, ensure that the new cluster address has been registered with DNS, and resolves to the external IP addresses of all the Application Server nodes in the cluster.

1. **SSH into the Master REAS VM** - SSH into the Master REAS VM (see above for credentials)
2. **Change the Cluster Address and Regenerate Certificates** - Execute the following command replacing `example.com` with the DNS registered FQDN of the cluster.

   ```
   /root/change-cluster-address.sh --regenerate-certs example.com
   ```

   Note: that the “--regenerate-certs” argument will regenerate the REAS Load Balancer certificates such that they are self-signed and contain the new cluster address. The short form of the “--regenerate-certs” script arguments is “-r”.

   Be aware that the existing certificates will be overwritten!

3. **Restart all REAS nodes in the cluster** - SSH into the external address of each REAS node in the cluster and restart the REAS service by executing the following command.

   ```
   service reas restart
   ```

---

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

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.

![Multi-Node Deployment Diagram](image-url)

**Figure 4. Multi-Node Deployment**

### Required Interfaces

The diagram (Figure 10) 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 its 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:** Figure 10 shows the LANs “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 10. Multi-Node Multi-NIC

OVA Deployment

**Note:** As mentioned earlier, deploying the OVA will **ALWAYS** create a VM hosting the REAS and the Media Broker.

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

As the OVA being deployed will host just the Media Broker in this multi-node topology, post-deployment, the REAS service should be disabled. 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:** These instructions can be repeated to install additional Media Brokers.

**Note:** 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 VMare 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 (ex. RE Mobile-10.6.1.10000-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 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.

   Remote Expert Mobile – Large Machine

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

   Ensure the Large Machine configuration supported by the capacity of your VMware Host / 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): Configure the template network details.

   Note: IP addresses are assigned during installation. These addresses CANNOT be changed once assigned. If you assign an incorrect address, or wish to change an IP address, you must re-install the node.
a. Node Configuration (REMB)

I. **Node Type** – All Media Broker VMs being created require the Node Type to be set to **Master**.

   Note that the Media Broker will need to be manually added into the Web Gateway cluster’s configuration. This is described in Step 18 below - Configuring the Web Gateway Cluster with the Media Broker.

II. **Cluster Address** - This property is only required when installing a master REAS node. As the VM being installed will host just a Media Broker, this field should be ignored.

III. **Master Node Address** - This property is only required when installing a slave REAS node. As the VM being installed will host just a Media Broker, this field should be ignored.

b. Network Time Configuration (REMB)

When installing a multi-node cluster, NTP must be configured by selecting the “Use Network Time Server?” checkbox and specifying an appropriate NTP server address e.g. time1.google.com

c. Network Name Resolution (REMB)

   **Host Name** - Specify the desired hostname of the VM being installed. This should be an FQDN.

   **DNS Server 1** - This is a mandatory field. Enter the address of DNS server that the RE Mobile VM should use.

   **DNS Server 2** - The second DNS server is an optional field.

c. External Network Configuration (REMB)

As mentioned earlier, configuring the external network is mandatory for each VM being created.

I. **External IP Address** - 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 selected on the previous screen.

II. **External Network Mask** - Enter the required network mask (e.g. 255.255.255.0) for the LAN associated with the External interface.

III. **External Gateway** - Enter the IP address of the External interface’s default network gateway.

   Note that this is NOT related to the REAS.

d. Internal Network Configuration (REMB)

As described earlier, the Media Broker will be configured with 2 NICs - External and Internal. In order to enable and configure the Internal interface, the **Use Internal Network** checkbox **MUST** be checked.

1. **Internal IP Address** - 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 selected on the previous screen.

2. **Internal Network Mask** - Enter the required network mask (e.g. 255.255.255.0) for the LAN associated with the Internal interface.

3. **Internal Gateway IP Address** - Enter the IP address of the Management interface’s default gateway.

   Note that this is NOT related to the REAS.
4. **Internal Gateway Remote Network (CIDR format)** - If the Application Server is expected to communicate with entities on a different network via this interface, the IP address range (encompassing the other entities) on the other network should be entered (in CIDR format) e.g. 10.10.0.0/24. Configuring this field will cause a static route to be added to the VM’s network routing table. This is not required. Therefore, this field should be left blank.

E. **Management Network Configuration (REMB)**

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.

**Step 14 (REMB):** Review the summary, check the box to power on the VM once deployment has completed, and click **Finish** to begin deployment.

**Step 15 (REMB):** OVA installation will now proceed – wait for it to complete.

**Step 16 (REMB):** Post install server access.

On first boot of your new VM, the OS and RE Mobile applications will be configured according to the details entered when deploying the OVA.

As such, the first boot of the new VM will take longer than a normal boot. 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: root
Password: changeit

Disable the REAS by executing the following command:

```
/opt/cisco/REAS-10.6.1.10000-x/REAS/resources/disable-service.sh
```

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

Navigate to the Remote Expert Mobile Administration web console at:

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

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 Media Broker’s “Internal” interface. The Web Gateway will use this address on the Media Broker to configure and control it.

c. Add a new “SIP Network” record.

d. **Local Address CIDR** – This is the address range the Media Broker will bind to for RTP communications on the SIP Network. Set this to the IP address of the “Internal” interface in CIDR format i.e. `<IP-Address>/32`

e. **Start/Finish Port Ranges** – This is the port range the Media Broker will bind to on the SIP Network e.g. 17000 – 17500

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

*Number of concurrent calls the Media Broker 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 e.g. 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 e.g. 16000

j. **Local Address & Port** – This is the IP address and port the Media Broker will bind to in order to receive RTP traffic from WebRTC clients e.g. 16000

k. As the media Broker 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 e.g. 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 Media Broker.

   **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 Step18 (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** section below.
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.

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” to 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 3 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 server’s IP address, but could have been changed. 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 Management Console, and you can manage the certificates for multiple Server Groups. The 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 during 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.

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 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. Open the Management Console by pointing your browser at Error! Hyperlink reference not valid. The default username and password are administrator and administrator respectively (these should be changed).

2. In the 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 and select ID Certificates.

5. Select the identity certificate group that you want to work with.

6. Click Generate Keypair.

7. 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.

8. 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.

9. Enter the expiry date, in the form yyyy-mm-dd. For example: 2015-03-20.

10. Enter the security password.

11. 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. In the Management Console, 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:

   ![Generated CSR](image)

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**.
Once the certificate is imported, the window is updated to reflect any changed certificate details, such as the issuer DN and the expiry date.

8. 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. In the Management Console, 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:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for this SCEP configuration</td>
</tr>
<tr>
<td>URL</td>
<td>The SCEP Server CGI URL. A typical value for an EJBCA server might be something like: <a href="http://ejbca.example.com:8080/scepraserver/scep/pkiclient.exe">http://ejbca.example.com:8080/scepraserver/scep/pkiclient.exe</a></td>
</tr>
<tr>
<td>Profile</td>
<td>Enter the value of the SCEP profile, or identity, that you want to use</td>
</tr>
<tr>
<td>Subject DN Prefix</td>
<td>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=Cafex,OU=Test”, the subject DN might be something like “C=GB,O=Cafex,OU=Test,CN=example.com”.</td>
</tr>
</tbody>
</table>

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".
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.

The CSR is generated, sent to the SCEP server, signed, returned, and imported into the identity certificate group directory.

5. The updated identity certificate group directory is then copied automatically to each Application Server and Load Balancer in the Server Group.
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. In the Management Console, 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 whose certificate you want to import, and the security password.
7. Open the certificate from the unknown CA 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 REA must also have an identity certificate containing the CN of that server. 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. In the Management Console, 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:
   - If you want the certificate to be signed by the SCEP server, click SCEP Sign Certificate.
   - If you want the certificate to be signed by a third-party CA, generate a CSR (see "Generating a CSR"), 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. In the Management Console, 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:
   - If you want the certificate to be signed by the SCEP server, click SCEP Sign Certificate.
   - If you want the certificate to be signed by a third-party CA, generate a CSR (see "Generating a CSR" on page 102), 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

1. If you want to create a backup copy of a certificate signed by a third-party CA, you can do so by exporting it.
2. In the 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 and select ID Certificates.
5. Select the identity certificate group that you want to work with.
6. Select the certificate entry of the identity certificate that you want to export.
7. Click Export.
8. Enter the security password. A dialog containing the certificate text is displayed.
9. Copy the text and paste it into a text editor, then save the file.
10. Click Cancel to close the dialog.

Removing a trust certificate

You would typically remove a trust certificate to prevent TLS connections from machines that use identity certificates signed by a specific CA that you no longer trust.

1. In the Management Console, 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, you can log in to the operating system using the following default credentials:

- **username:** root  
- **password:** changeit

These credentials should be changed upon install.

**Remote Expert Mobile Administration Console**

The credentials for the Remote Expert Mobile Administration Interface, available at `https://<target-vm>:8443/web_plugin_framework/webcontroller` are:

- **username:** admin  
- **password:** admin

These credentials should be changed upon install.

**RE Mobile Gateway Configuration – Outbound SIP Server**

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>` (e.g. 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:

- First, all UP servers are added in a random order.
- 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.
Expert Assist Configuration – Consumer Access Number Regex

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 (e.g. 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. Navigate to the Remote Expert Mobile Administration web console at:
   https://<reas-address>:8443/web_plugin_framework/webcontroller

2. Authenticate with the credentials:
   
   Username: admin
   Password: admin

3. Navigate to the Expert Assist tab and click the General Administration menu.
4. Edit the Consumer Access Number Regex field with a regular expression suitable for your deployment environment. e.g. To only allow calls to the destination: sip:60017@100.1.0.100, enter the regex: ^sip:60017@100.1.0.100$

5. 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 – Image Quality Scale Factor

Remote Expert Assist can be configured to configure the quality of the screen share seen within the Agent Console.

This "Image Quality Scale Factor" is a configuration item of RE Mobile and can be changed via the Expert Assist Administration page on the Web Plugin Framework web console.

1. Navigate to the Remote Expert Mobile Administration web console at:

   https://<reas-address>:8443/web_plugin_framework/webcontroller
2. Authenticate with the credentials:
   
   Username: admin
   
   Password: admin

3. Navigate to the Expert Assist tab and click the General Administration menu.
   
   The property is called "Image Quality Scale Factor" and is defined within a range of 0 to 1, with the default setting being 0.5. Setting this to 1 will apply no scaling, however will require more bandwidth.

Expert Assist Configuration – Enabling UUI Data

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 that 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 Plugin Framework web console.

1. Navigate to the Remote Expert Mobile Administration web console at:
   
   https://<reas-address>:8443/web_plugin_framework/webcontroller

2. Authenticate with the credentials:
   
   Username: admin
   
   Password: admin

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

You can configure how hold is rendered to endpoints using the settings in the proxy.properties file on each of the REM Media Broker servers. 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

- video.hold.image.path
— Video hold image path - image must be in PNG format

- audio.hold.on
  — true|false
  — Whether or not video on hold is enabled

**Expert Assist Configuration – Call Admission Control**

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 from the Remote Expert Mobile web plugin framework: Gateway -> General Administration page.

Note that Call Admission Control is enabled “out of the box”, with Max Load Factor set to ”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.

Below are configurable fields explained:

| 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).
| 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.

Note that a value of “0” in this field will disable this function i.e. no check will be made.
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.

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://<reas-address>: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://<reas-address>: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.
Integrating Remote Expert Mobile

If you’ve 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. Navigate to the Remote Expert Mobile Administration web console at:

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

2. Authenticate with the credentials:

   Username: admin
   Password: admin

3. 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 e.g.
     - 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 e.g.

- 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`.
  - When a user logs in via 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.
  - Consider disabling this local user for production deployments.

- A list of Finesse Servers

  This configuration is relevant only to Contact Center deployments

  - The RE Mobile Finesse gadgets use this list of servers to authenticate both Agents and Supervisors.

  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 credentials to Expert Assist, which will attempt to contact the first server in this list asking it to validate the user’s credentials. The next server in the list will only be contacted if the current server does not respond (e.g. if the server is offline). If the current server responds, Expert Assist will either give permission to the gadget to perform the user’s requested operation, or deny it permission, based on the response received from the server.

  - In a clustered Finesse server environment, the Gadget may be configured with many Finesse Servers and may authenticate with any of them.
  - Click the Add button and enter the HTTP(S) URL of each Finesse Server (e.g. `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 Remote Expert Mobile Expert Assist Web Console User Guide for more details.
  - Click the Add button and enter the HTTP(S) URL of each Call Manager (e.g. `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.

4. 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

1) Set **Trust All Certificates** to true (only recommended for trials)

2) Set **Trust JDK Certificates** to true (this will only work if Finesse/AXL are signed by a well known CA) or

3) 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 10.6(2) - Expert Assist Web Console User Guide” for information on using these applications.

### Configuration Steps

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Call Manager address(es) for AXL authentication</td>
<td>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.</td>
</tr>
<tr>
<td>Configure outbound SIP routing</td>
<td>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.</td>
</tr>
<tr>
<td>Test</td>
<td>See “Testing the Agent Console” below.</td>
</tr>
<tr>
<td>Inbound calling restrictions (optional)</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Testing the UC Integration

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://<reas-address>:8443/expertassist/agent](https://<reas-address>:8443/expertassist/agent)
b. Enter the credentials of a Call Manager 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>

   e.g., 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

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 10.6(2) - Finesse Gadget User Guide” for information on using these gadgets.
Configuring the Cisco Remote Expert Mobile Solution

**Configuration Steps**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure inbound calling</td>
<td>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:</td>
</tr>
<tr>
<td></td>
<td>• Configure an inbound number must be defined allowing RE Mobile consumers to call into Agents.</td>
</tr>
<tr>
<td></td>
<td>• Configure CCE/CCX to route the configured inbound number to one or more Agent queues.</td>
</tr>
<tr>
<td>Finesse Server Trust Management</td>
<td>Enable HTTPS communication from the Finesse Server(s) to the REAS – See “Finesse Server Trust Management” below.</td>
</tr>
<tr>
<td>Configure gadgets in Finesse</td>
<td>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 &amp; Supervisor Gadgets within the Finesse Server” section below for details.</td>
</tr>
<tr>
<td>Configure RE Mobile with Finesse Server Addresses for authentication</td>
<td>Configure the addresses of the machines within the Finesse server cluster via the Web Gateway’s administration console – See the “Configuring the Agent &amp; Supervisor Consoles within the RE Mobile Application Server” section below for details.</td>
</tr>
<tr>
<td>Configure outbound SIP routing</td>
<td>RE Mobile will route SIP messages via one or more CUBEs. See “RE Mobile GatewayConfiguration – Outbound SIP Server” above for more information on how to configure these addresses.</td>
</tr>
<tr>
<td>Enable SSLv2Hello (pre 10.6 Finesse)</td>
<td>Enable SSLv2Hello on REAS when integrating with Finesse Server versions prior to 10.6 – See the “Enable SSLv2Hello Support” section below for details.</td>
</tr>
<tr>
<td>Test</td>
<td>See “Testing the Finesse Gadget” below.</td>
</tr>
<tr>
<td>Inbound calling restrictions (optional)</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 e.g.

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

And to return to default behaviour, invoke the `<REAS_INSTALL_DIR>/resources/disable-sslv2.sh` script on each REAS host in the cluster e.g.

```
[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 above 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:


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

```xml
<tab>
  <id>EA</id>
  <label>Expert Assist</label>
  <gadgets>
    <gadget>https://<reas-address>:8443/finesse_assist_gadget/FinesseAssist.xml?finesseVersion=10.5.1
  </gadget>
</tab>
```

**Note:** Please ensure that the finesseVersion request parameter in the URL above is modified to your version of Finesse. If a value of 10.6.1 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

```xml
<tab>
  <id>EAS</id>
  <label>Expert Assist Supervisor</label>
</tab>
```
<gadgets>
  <gadget>https://<reas-address>:8443/finesse_assist_admin_gadget/FinesseAssistAdmin.xml</gadget>
</gadgets>

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>

   e.g., 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 as shown in the diagram below.

By only making specific REAS URIs publically visible, results in clients (in the Consumer Network) only having access to the server resources they need, while all others are protected.

![Diagram of Reverse Proxy Installation](image)

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

<table>
<thead>
<tr>
<th>Path</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/csdk-sample/*</td>
<td>HTTP(s)</td>
<td>Client SDK sample application.</td>
</tr>
<tr>
<td>/gateway/csdk-sdk.js</td>
<td>HTTP(s)</td>
<td>Web SDK assets.</td>
</tr>
<tr>
<td>/gateway/csdk-presence.js</td>
<td>HTTP(s)</td>
<td>Web SDK assets.</td>
</tr>
<tr>
<td>/gateway/csdk-aed.js</td>
<td>HTTP(s)</td>
<td>Web SDK assets.</td>
</tr>
<tr>
<td>/gateway/csdk-common.js</td>
<td>HTTP(s)</td>
<td>Web SDK assets.</td>
</tr>
<tr>
<td>/assistserver/defaultUIResources/*</td>
<td>HTTP(s)</td>
<td>Default UI used by iOS clients.</td>
</tr>
<tr>
<td>/assistserver/img/*</td>
<td>HTTP(s)</td>
<td>Some common graphical resources.</td>
</tr>
<tr>
<td>/assistserver/consumer</td>
<td>HTTP(s)</td>
<td>Servlet used to provide clients with a session.</td>
</tr>
<tr>
<td>/assistserver/sdk/web/consumer/*</td>
<td>HTTP(s)</td>
<td>Web SDK assets.</td>
</tr>
<tr>
<td>/assistserver/sdk/web/shared/*</td>
<td>HTTP(s)</td>
<td>Web SDK assets.</td>
</tr>
<tr>
<td>/gateway/adapter.js</td>
<td>HTTP(s)</td>
<td>Web SDK assets.</td>
</tr>
<tr>
<td>/assistserver/topic</td>
<td>WebSocket</td>
<td>WebSocket used for screen share, annotations ...etc.</td>
</tr>
</tbody>
</table>
The following specifically relates to the RE Mobile consumer-side sample application URIs.

<table>
<thead>
<tr>
<th>Path</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/assistsample/*</td>
<td>HTTP(s)</td>
<td>Expert Assist sample client application.</td>
</tr>
</tbody>
</table>

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

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

Supported features

1. **SAN with Fibre interconnect** - Use of a SAN with Fibre interconnect, rather than a NAS, is recommended in order to maximize the transfer speed.

2. Incremental VMware Backups - If incremental backups are to be enabled, ensure that you follow the VMware Guides on 1st & 3rd Party Backup Solutions.

Unsupported features

1. **VMware fault tolerant mode** - VMware fault tolerant mode is not supported (because the Remote Expert Mobile uses multiple cores).

2. **vMotion** - vMotion has not been tested with Remote Expert Mobile.

* **NOTE**: VMware snapshots are not supported and will cause performance issues
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 is service affecting. The RE Mobile cluster will be unavailable whilst the upgrade is taking place.

Upgrade

It is possible to upgrade from release 10.6(1) to this new release using this procedure. 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:

5. Stop the REAS and REMB services on all nodes.
   
   See “Stopping Services” below.

6. Run the upgrade script on each of the nodes in the following order:
   
   d. REAS Master
   
   e. REAS Slave
   
   f. REMB – update each in turn in any order
   
   See “Upgrading a Node” below.

Stopping Services

For nodes running REAS, run:

```bash
service reas stop
```

For nodes running REMB, run:

```bash
service media_broker stop
```

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 (e.g. REM-upgrade-10.6.2.10000-n.tar.gz) to the node's tmp directory e.g.

   ```bash
   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

- Confirm upgrade
- Accept license terms.
- For Master REAS nodes the following additional steps are included
  - Enter REAS administrator username/password: (default is administrator/administrator)
  - Enter REAS REST username/password (default is admin/admin)
- Confirm shutdown of service(s)
  - Note: this step will print FAILED if the services have already been stopped, the message can be safely ignored.
- The installation will complete and the REAS and/or REMB service(s) will be automatically restarted.

4. 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
+--- 10.6.1.1.10000-8
 |   +---BIN
 |   |   +---CSDK
 |   |   +---REAS
+--- 10.6.2.10000-2
 |   +---BIN
 |   |   +---CSDK
 |   |   +---REAS
+--- bin->10.6.2.10000-2/BIN
```

**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. Run the rollback script on each of the nodes in the following order:

   a. REAS Master
   b. REAS Slave
   c. REMB – roll back each in turn in any order
See “Rolling back a Node” below.

Rolling back a node

To roll back a node to a previous version of RE Mobile, invoke the /opt/cisco/bin/rollback.sh script.

- For a list of options this script provides, use:
  
  /opt/cisco/bin/rollback.sh --help

- To list the versions of RE Mobile that have previously been installed on a node use:
  
  /opt/cisco/bin/rollback.sh -l

- To roll back to a previous version, use:
  
  /opt/cisco/bin/rollback.sh -v <version>

  e.g. /opt/cisco/bin/rollback.sh -v 10.6.1.10000-8 will roll back to RE Mobile 10.6.1.10000-8

Checking the RE Mobile Version

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

- Open the following url in a browser:
  
  — https://<reas cluster name>:8443/web_plugin_framework/webcontroller/gateway/

- Provide credentials (default is admin/admin)

- The page will display the RE Mobile version number e.g.

  — Gateway Administration Portal (Product Version: 10.6.2.10000-2)
Acronym List

- **CIDR** - Classless Inter-Domain Routing
- **CODEC** – “coder-decoder” encodes a data stream or signal for transmission and decodes it for playback in voice over IP and video conferencing applications.
- **CSDK** - Remote Expert Mobile Client SDKs. Includes three distinct SDKs for iOS, Android and Web/JavaScript developers.
- **CUBE** – Cisco Unified Border Element, a Cisco session border controller used in contact center and unified communications solutions
- **CUCM** – Cisco Unified Communications Manager or Unified CM
- **CUCS** – Cisco Unified Computing System servers
- **CVP** - Cisco Unified Voice Portal
- **G.711** – PCMU/A 8-bit audio codec used for base telephony applications
- **G.729a** – low bit rate audio codec for VoIP applications
- **H.264** – video codec. H.264 is the dominant video compression technology, or codec, in industry that was developed by the International Telecommunications Union (as H.264 and MPEG-4 Part 10, Advanced Video Coding, or AVC). Cisco is open-sourcing its H.264 codec (Open H.264) and providing a binary software module that can be downloaded for free from the Internet. Cisco will cover MPEG LA licensing costs for this module.
- **Opus** – low bit rate, high definition audio codec for VoIP applications. Opus is unmatched for interactive speech and music transmission over the Internet, but is also intended for storage and streaming applications. It is standardized by the Internet Engineering Task Force (IETF) as RFC 6716 which incorporated technology from Skype’s SILK codec and Xiph.Org’s CELT codec (www.opus-codec.org)
- **NACK** – Negative Acknowledgement. NACK is used by the receivers of video to indicate the loss of one or more RTP packets as part of the base mechanisms of the Real-time Transport Control Protocol (RTCP). This enables the sender to resend video packets to handle packet loss over the Internet or poor network conditions.
- **PCCE** - Cisco Packaged Contact Center Enterprise (Packaged CCE)
- **PLI** – Packet Loss Indication is another feedback mechanism of the Real-time Transport Control Protocol (RTCP) which enables the sender to resend keyframe packets to re-establish a full video picture when communicating over the Internet or poor network conditions.
- **REAS** – Remote Expert Mobile Application Server
- **REMB** – Remote Expert Mobile Media Broker
- **RTP** – Real-time Transport Protocol
- **RTCP** – Real-time Transport Control Protocol
- **UC** – Unified Communications
- **UCCE** – Cisco Unified Contact Center Enterprise (Unified CCE)
- **UCCX** - Cisco Unified Contact Center Express (Unified CCX)
- **VP8** – video codec. VP8 is a video compression format owned by Google. Google remains a staunch supporter of VP8 after buying On2 Technologies in 2010. Google then released VP8 software under a BSD-like license as well as the VP8 bitstream specification under an irrevocable license and free of royalties. VP8 is roughly equivalent in processor usage, bandwidth and quality as H.264.
- **WebRTC** – Web Real Time Communications for plugin-less communications