



# Cisco Remote Expert Smart Solution 1.8 Implementation Guide

---

August 21, 2013

<b>1</b>	<b>Purpose .....</b>	<b>9</b>
<b>2</b>	<b>Prerequisites.....</b>	<b>10</b>
<b>2.1</b>	<b>Hardware, Software and Licensing.....</b>	<b>10</b>
<b>2.2</b>	<b>Infrastructure Prerequisites.....</b>	<b>10</b>
2.2.1	Solution Dial Plan .....	10
2.2.2	Expert Skill-Groups.....	11
2.2.3	Agent/Expert Workflows.....	11
2.2.4	Automatic Call Distributor Call Flows/Scripting.....	11
2.2.5	Digital Graphics Assets.....	11
<b>3</b>	<b>Cisco Remote Expert Smart Solution Functional Architecture .....</b>	<b>12</b>
<b>3.1</b>	<b>Data Center .....</b>	<b>12</b>
3.1.1	Interactive Experience Manager (IEM) .....	13
3.1.2	Remote Expert Manager (REM).....	14
<b>3.2</b>	<b>Expert Location .....</b>	<b>14</b>
3.2.1	Direct Connect .....	15
<b>3.3</b>	<b>Customer Location .....</b>	<b>15</b>
3.3.1	Interactive Experience Client (IEC) 4610.....	15
<b>4</b>	<b>Implementation Summary .....</b>	<b>17</b>
<b>5</b>	<b>Video Endpoint Provisioning.....</b>	<b>18</b>
<b>5.1</b>	<b>Licensing.....</b>	<b>18</b>
5.1.1	Cisco TelePresence EX60 and EX90 Series .....	18
5.1.2	Cisco TelePresence CTS-500 Series .....	18
<b>5.2</b>	<b>Firmware.....</b>	<b>18</b>
<b>5.3</b>	<b>Component Checkpoint: Verify your work .....</b>	<b>19</b>
5.3.1	Verify Touchpanel Information .....	19
5.3.2	Browse to Endpoint Administration Page .....	19
5.3.3	SSH To Endpoint Command Line Interface .....	19

<b>6</b>	<b>Unified Communication Manager Configuration for Remote Expert.....</b>	<b>20</b>
<b>6.1</b>	<b>General CUCM Configuration.....</b>	<b>20</b>
6.1.1	Audio Codec Preference List.....	20
6.1.2	SIP Trunk configuration .....	21
6.1.3	Route Pattern configuration .....	23
6.1.4	Disable Music On Hold (MOH) .....	23
6.1.5	Conference Bridge.....	24
<b>6.2</b>	<b>Device Specific Configuration.....</b>	<b>25</b>
6.2.1	Cisco TelePresence System (CTS) Endpoints.....	25
6.2.2	EX Endpoints .....	26
<b>6.3</b>	<b>CTI Specific Configuration.....</b>	<b>26</b>
6.3.1	Application User Accounts.....	26
6.3.2	End User Accounts .....	28
<b>6.4</b>	<b>Component Checkpoint: Verify your work .....</b>	<b>30</b>
6.4.1	Make video calls .....	30
<b>6.5</b>	<b>Troubleshooting.....</b>	<b>30</b>
<b>7</b>	<b>Unified Contact Center Enterprise (UCCE) Configuration Specifics for Remote Expert...</b>	<b>31</b>
<b>7.1</b>	<b>UCCE Installation Pre-requisites .....</b>	<b>31</b>
7.1.1	ICM Setup Program.....	31
7.1.2	Creating an ICM Instance .....	31
7.1.3	Configure Domain Manager .....	31
<b>7.2</b>	<b>UCCE Components.....</b>	<b>33</b>
7.2.1	Router Installation .....	33
<b>7.3</b>	<b>Logger Installation.....</b>	<b>33</b>
7.3.1	Logger Configuration .....	33
7.3.2	Admin Workstation (AW) Installation .....	34
7.3.3	Admin Workstation (AW) Configuration.....	35

7.3.4	Peripheral Gateway (PG) Installation .....	49
7.3.5	JTAPI Client Installation.....	51
7.3.6	CTI Server Installation.....	52
7.3.7	CTI OS Server Configuration .....	53
7.3.8	ICM Script .....	54
<b>7.4</b>	<b>Component Checkpoint: Verify UCCE component integration.....</b>	<b>55</b>
<b>7.5</b>	<b>Troubleshooting.....</b>	<b>55</b>
7.5.1	Service Temporary Unavailable message displayed instead of the Login page.....	55
7.5.2	Unified CCE Admin does not Display Properly in IE9 .....	56
7.5.3	Logger processes crashes after upgrade to SQL Server 2008 R2.....	56
7.5.4	SQL Server 2008 R2 fails registry key validation.....	57
7.5.5	Un-Installing SQL Server 2005 32 bit and Installing SQL Server 2008 64 bit.....	57
<b>8</b>	<b>Cisco Agent Desktop Services.....</b>	<b>59</b>
<b>8.1</b>	<b>Configuration.....</b>	<b>59</b>
8.1.1	Unified CM SOAP AXL Access.....	60
8.1.2	Unified Communications Manager.....	61
8.1.3	CTI Server (Unified CM).....	62
8.1.4	CTI OS .....	63
8.1.5	ICM Admin Workstation Distributor.....	64
8.1.6	ICM Admin Workstation Database.....	65
8.1.7	Admin Workstation computer .....	66
8.1.8	Recording and Statistics Database Configuration.....	66
8.1.9	Recording and Statistics Service Database .....	69
8.1.10	Restore Backup Data.....	70
8.1.11	CAD-BE Servers.....	70
8.1.12	VoIP Monitor Service.....	71
8.1.13	Services Configuration.....	72

8.1.14	SNMP Configuration.....	73
8.1.15	Thin Client Environment.....	74
8.1.16	Replication Setup .....	74
8.1.17	Modifying Configuration Settings.....	76
<b>8.2</b>	<b>Licensing CAD 9.0 .....</b>	<b>77</b>
8.2.1	Obtaining a License Account.....	77
8.2.2	Using Unified CCE License Administration.....	77
<b>8.3</b>	<b>Component Checkpoint.....</b>	<b>78</b>
<b>9</b>	<b>Cisco Agent Desktop Client Configuration.....</b>	<b>79</b>
<b>9.1</b>	<b>CAD client installation .....</b>	<b>79</b>
9.1.1	Installing Desktop Administrator .....	79
9.1.2	Installing Agent Desktop and Supervisor Desktop.....	79
9.1.3	Installation Notes .....	79
9.1.4	To reconfigure CAD client installation programs: .....	79
<b>9.2</b>	<b>Workflow Administrator .....</b>	<b>80</b>
<b>9.3</b>	<b>Component Checkpoint.....</b>	<b>86</b>
<b>10</b>	<b>VXML Gateway Configuration.....</b>	<b>87</b>
<b>10.1</b>	<b>IOS Configuration .....</b>	<b>87</b>
<b>10.2</b>	<b>Component Checkpoint: Verify VXML GW operation .....</b>	<b>95</b>
10.2.1	Show commands.....	95
10.2.2	Debug Commands .....	95
<b>11</b>	<b>Customer Voice Portal Server Configuration.....</b>	<b>97</b>
<b>11.1</b>	<b>CVP Media Server Configuration .....</b>	<b>97</b>
<b>11.2</b>	<b>CVP Configuration.....</b>	<b>99</b>
11.2.1	CVP Operations Console.....	100
11.2.2	CVP Call Server .....	100
11.2.3	VXML Gateway.....	101

11.2.4	CVP Media Server .....	102
11.2.5	Dialed Number Pattern .....	102
11.2.6	Miscellaneous .....	103
<b>11.3</b>	<b>Solution Checkpoint: Verify Call Routing .....</b>	<b>104</b>
<b>12</b>	<b>Remote Expert Manager Hardware Provisioning .....</b>	<b>105</b>
<b>12.1</b>	<b>Host Provisioning For Virtual Deployments .....</b>	<b>105</b>
<b>12.2</b>	<b>Host Platform Considerations for Remote Expert Manager High Availability .....</b>	<b>106</b>
<b>13</b>	<b>Interactive Experience Manager (IEM) Installation and Configuration .....</b>	<b>107</b>
<b>13.1</b>	<b>Install and Configure IEM Software .....</b>	<b>107</b>
<b>13.2</b>	<b>IEM High Availability .....</b>	<b>107</b>
<b>13.3</b>	<b>Component Checkpoint: Verify Installation and Initial Configuration .....</b>	<b>107</b>
<b>14</b>	<b>Interactive Experience Client (IEC) Provisioning and Configuration .....</b>	<b>108</b>
<b>14.1</b>	<b>Deploy One or More Customer Pods Featuring an IEC-4600 Series Client .....</b>	<b>108</b>
<b>14.2</b>	<b>Component Checkpoint: Verify Installation and Initial Configuration .....</b>	<b>108</b>
<b>15</b>	<b>Remote Expert Manager Installation and Configuration .....</b>	<b>109</b>
<b>15.1</b>	<b>Install and Configure REM Software .....</b>	<b>109</b>
<b>15.2</b>	<b>Deploy Default Branding Assets .....</b>	<b>109</b>
<b>15.3</b>	<b>REM High Availability .....</b>	<b>109</b>
<b>15.4</b>	<b>Component Checkpoint: Verify Installation and Initial Configuration .....</b>	<b>109</b>
<b>15.5</b>	<b>Media Server Identification/Installation .....</b>	<b>110</b>
<b>15.6</b>	<b>Component Checkpoint: Verify Installation &amp; Configuration of Media Server .....</b>	<b>110</b>
<b>16</b>	<b>Basic REM Operational Configuration Using the Remote Expert Administration Console (REAC) .....</b>	<b>111</b>
<b>16.1</b>	<b>Prerequisites .....</b>	<b>111</b>
<b>16.2</b>	<b>Introducing REAC .....</b>	<b>111</b>
16.2.1	Configure Locales .....	112
16.2.2	Configure Expert Types and Pilot DNs for Skill-Groups .....	112

16.2.3	Configure Contact Center Agents as Remote Experts .....	112
16.2.4	Upload and Designate Videos on Demand .....	113
16.2.5	Upload and Designate Static Graphic Images for the Customer Pod .....	113
16.2.6	Upload and Documents for Sharing with the Customer Pod.....	113
16.2.7	Create a Customer Feedback Survey.....	113
16.2.8	Register Customer Pod with REM .....	113
<b>16.3</b>	<b>Component Checkpoint: Verify REM Operational Configuration.....</b>	<b>113</b>
<b>17</b>	<b>DirectConnect Installation and Configuration and Integration with Cisco Agent Desktop (CAD) .....</b>	<b>115</b>
17.1	Install and Configure Direct Connect Software .....	115
17.2	Component Checkpoint: Verify Direct Connect Configuration .....	115
<b>18</b>	<b>Solution Checkpoint: Verify Basic System Functionality .....</b>	<b>116</b>
18.1	Prerequisites .....	116
18.2	Log into Cisco Agent Desktop as a Remote Expert .....	116
18.3	Initiate a Remote Expert Collaboration Session via the Collaboration Panel.....	117
18.3.1	Expected TelePresence Endpoint Behavior While the Session is In Queue.....	117
18.3.2	Expected Collaboration Panel Behavior While the Session is In Queue.....	118
18.4	Ready the Remote Expert, Answer an Incoming Call and Start a Remote Expert Session.....	118
18.5	Verify READ Video and Document Inventory.....	119
18.6	Preview and Share a Video with the Customer Pod.....	120
18.7	Preview and Print Documents at the Customer Pod .....	120
18.8	Use Direct Connect to Share an Application on the Agent Desktop with the Customer Pod.....	120
<b>19</b>	<b>Advanced Features .....</b>	<b>124</b>
19.1	MediaSense.....	124
19.1.1	CUCM Configuration.....	124
19.1.2	MediaSense API User Configuration.....	125

19.1.3	Prune Policy Configuration .....	125
19.1.4	MediaSense Server Configuration .....	126
<b>19.2</b>	<b>Cisco Unified Border Element (CUBE) .....</b>	<b>127</b>
19.2.1	CUBE/Forking Configuration .....	127
<b>19.3</b>	<b>Conferencing/Transfers .....</b>	<b>131</b>
19.3.1	MCU 4610 Configuration.....	131
<b>20</b>	<b>Specialized Customer Pod peripheral integration.....</b>	<b>132</b>
<b>21</b>	<b>Custom Branding the Remote Expert Smart Solution.....</b>	<b>133</b>
<b>22</b>	<b>References .....</b>	<b>134</b>



# 1 Purpose

---

This document is intended as a solution-level, step-by-step reference for technical professionals responsible for preparing, planning and implementing the Remote Expert Smart Solution for an Enterprise customer.

This document provides planning considerations and recommendations, but does not discuss all the foundational technologies, procedures and best practices for deploying the routing, switching, unified communications system, contact center applications, etc., required by the solution. Instead, it refers to detailed documents that discuss those technologies and implementation methods, while focusing on specific configuration and best practices for deploying them within the Cisco Remote Expert Smart Solution.

The Cisco Remote Expert Smart Solution is based on the integration of products and technology from Cisco and third-party vendors. References to third-party vendors' product and system documentation are offered where necessary. Although efforts have been made to confirm that these references are accurate, there may be instances in which changes to a vendor's product or design guidance make specific references in this guide out of date. Please contact Cisco if you find such disparities.

## 2 Prerequisites

### 2.1 Hardware, Software and Licensing

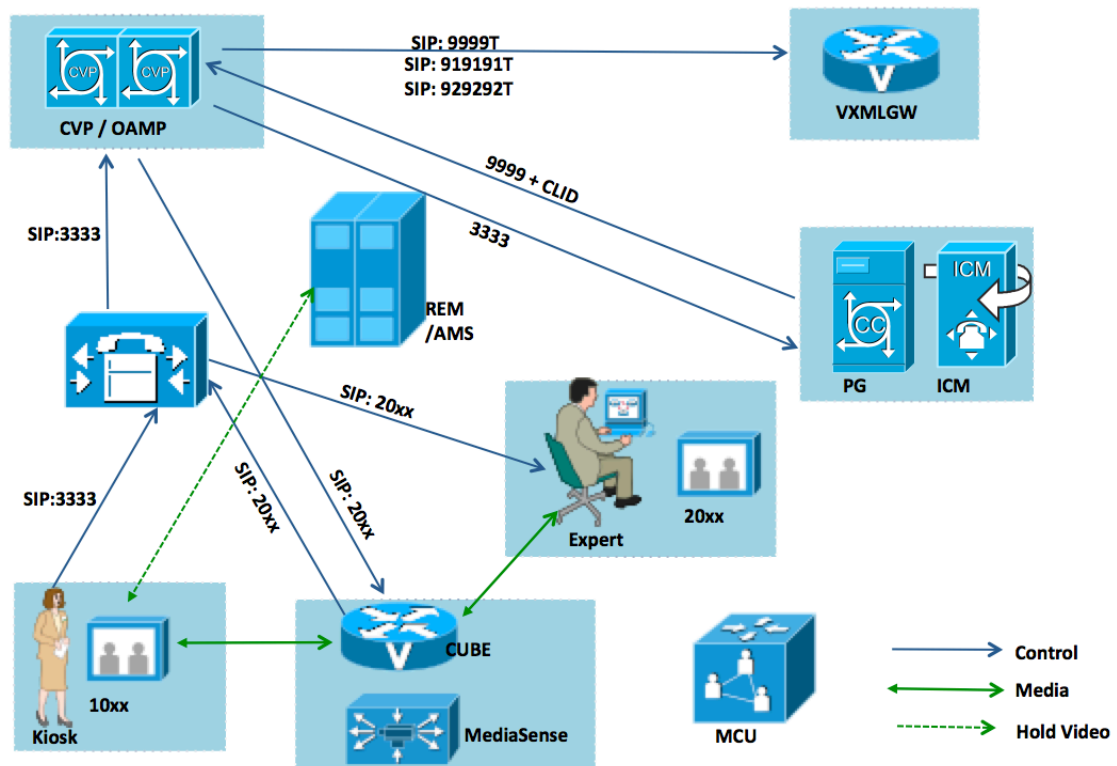
To ensure a smooth and successful Remote Expert Smart Solution deployment, please refer to the individual product requirements to verify that the necessary hardware, software and licensing prerequisites are in place before proceeding.

### 2.2 Infrastructure Prerequisites

Please be sure to coordinate with the Unified Communications (UC) and Contact Center (CC) administrators to gather and understand the following information about the UC/CC infrastructure. The Remote Expert Smart Solution requires certain capabilities exist within the UC/CC infrastructure. Also, certain information about the UC/CC infrastructure is required when installing and configuring the Remote Expert Manager (REM).

#### 2.2.1 Solution Dial Plan

Figure 1: Solution Dial Plan



### **2.2.2 Expert Skill-Groups**

It's a good practice to keep a list of the experts and their specific roles as in if they would be an agent or Administrator/Supervisor and also note down what is the kind of login/password scheme you would like to use for agent login at this point. This would help in constructing the configuration manager database, which we would be focusing on, in Chapter 6.

### **2.2.3 Agent/Expert Workflows**

Ensure you have installed the REM and have necessary URLs ready for the configuration. In addition, CAD admin needs to be installed on one of the administrator/supervisor desktops and the configuration is initiated from this CAD admin application.

### **2.2.4 Automatic Call Distributor Call Flows/Scripting**

On the Admin Workstation node, make sure the scripting utility is installed. Get familiar with the nodes in the utility, which becomes important when building the icm script. Also having the call flow and the dial-pattern map before hand helps in making sure the script is easy to build. Also, there is a monitor button on the script, which can be used to trace the call to a specific node when a UCCE call is made.

### **2.2.5 Digital Graphics Assets**

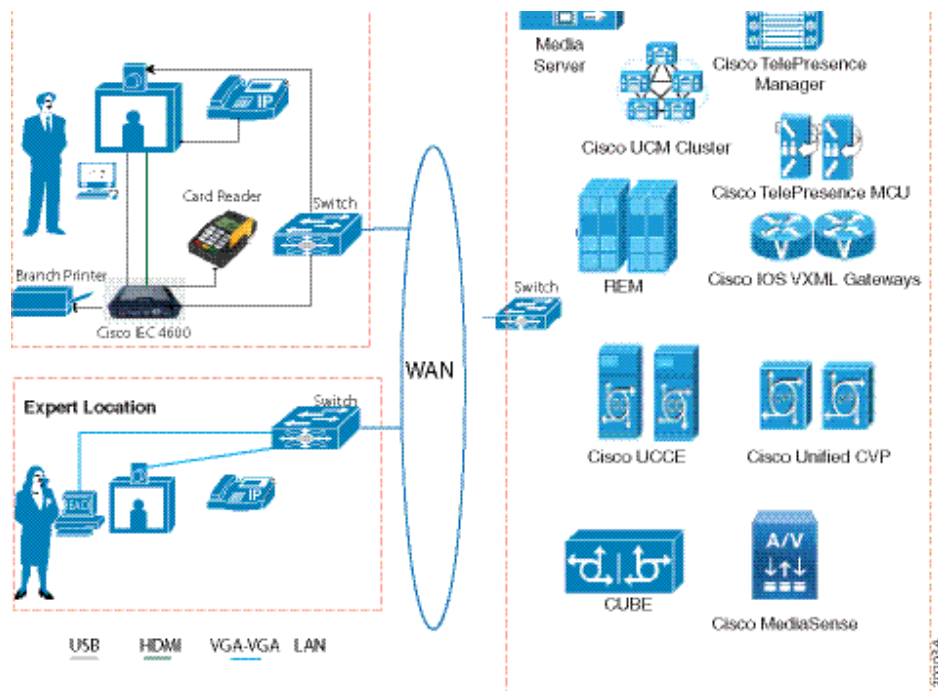
Custom branding assets will need to be designed, developed, tested in conjunction with the solution and approved by the enterprise customer before the solution can be placed into actual trials or production.

### 3 Cisco Remote Expert Smart Solution Functional Architecture

The Cisco Remote Expert Smart Solution consists of products from the Cisco Unified Communications Architecture and Interactive Services (iServices) product lines, as well as third-party products. As shown in Figure 2, these products are deployed at different physical and logical locations within the enterprise: at the customer locations, at the enterprise data center, and at the expert location.

This section lists the individual components of the solution and describes where these fit into the enterprise network.

Figure 2: Cisco Remote Expert Smart Solution Functional Architecture



#### 3.1 Data Center

A typical Cisco Remote Expert Smart Solution deployment may include the following components in the Data Center:

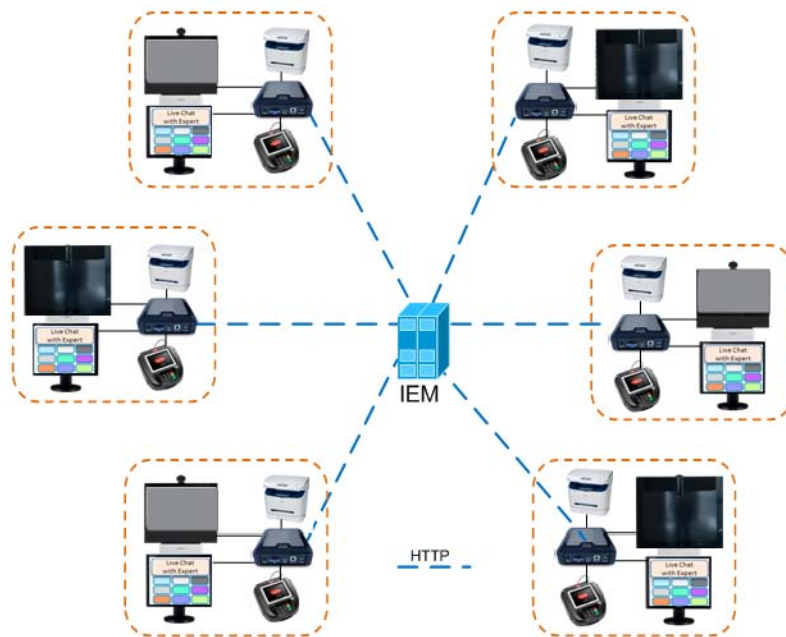
- Cisco Unified Communications Manager (UCM)
- (Optional) Cisco TelePresence Manager (CTM)
- (Optional) Cisco TelePresence Multimedia Conferencing Unit (MCU)
- Cisco Unified Contact Center Enterprise (UCCE) and companion components\*
- Cisco IOS® Voice XML (VXML) Gateway
- Cisco Unified Customer Voice Portal (CVP)

- Cisco Interactive Experience Manager (IEM)
- Cisco Remote Expert Manager (REM)
- Media server or content distribution solution such as Cisco Enterprise Content Delivery System (ECDS)
- (Optional) Cisco Unified Border Element (CUBE)
- (Optional) Cisco MediaSense for audio recording
- Server load balancer, such as the Cisco Application Control Engine (ACE) Module

### 3.1.1 Interactive Experience Manager (IEM)

The IEM is a centralized solution allowing configuration, control, and support of Interactive Experience Client (IEC) 4610 endpoints. Unlike traditional management servers, there's nothing to install on premises, and no software to upgrade. An on-premises version of the IEM is available to enterprises choosing to run the application in their data centers.

Figure 3: IEM Manages Multiple IEC endpoints



The IEM performs the following functions:

- Configuration - The IEM allows the administrator to manage the system behavior, such as desktop elements, window mode (customer pod vs. single-window vs. multiple-window), network settings, printing preferences, peripheral support, etc.
- Customer pod configuration - The customer pod mode refers to a full-screen mode of operation. Under this model, the customer pod will start with a predetermined Internet resource (a special web page, flash, or movie), and let the user navigate within a “walled garden” environment
- Logging and reporting - The IEC can be set up to log the traffic from the IEC devices, making it easy for the administrators to analyze the data and make access restriction decisions. This traffic

data collection and be performed in private mode with the administrator seeing the aggregate data only

- Policies - Policies provide an easy and flexible way of applying settings to a group of users or devices. For example, an administrator can apply a policy to use certain printer for certain section of the building, or restrict Internet access on some, but not other terminals.

For more information of IEM, refer to the [Cisco Remote Expert Manager 1.8 Installation Guide](#).

### 3.1.2 Remote Expert Manager (REM)

The REM is the platform that provides interactive experience during an immersive video call between a customer and a remote expert. The REM uses different call events and state information to run its intelligent logic for providing the interactive experience.

The REM solution encompasses following components:

- Remote Expert Agent Desktop (READ)
- Remote Expert Interactive Collaboration (REIC) application
- Remote Expert Service Control (RESC)
  - Tomcat/Apache based Web services
  - PostGRE-SQL based Data-Store
  - JTAPI Adapter for Cisco UCM Integration

Other components that REM relies on its functions are the following:

- Interactive Experience Manager (IEM)
- Interactive Experience Client (IEC)
- Media Server

REM is the core control system of the Cisco Remote Expert Solution that provides the collaboration feature that makes customer's interaction with the remote expert simpler and effective.

For more information about REM, please see the [Cisco Remote Expert Manager 1.8 Installation Guide](#).

## 3.2 Expert Location

A typical Cisco Remote Expert Smart Solution deployment may include the following components at the Expert Location:

- Cisco TelePresence System (CTS) 500 Series, EX60 or EX90 endpoints
- Agent workstation PC
- Collaborative workspace components installed on the agent workstation, including:
  - Cisco Agent Desktop
  - Direct Connect Application (included with the Cisco Remote Expert Smart Solution)

### 3.2.1 Direct Connect

Direct Connect is a software application running on the expert's workstation and provided as part of the Cisco Remote Expert Smart Solution. Direct Connect allows real-time collaboration between experts and customers using any enterprise application on the agent's workstation. These applications can be natively shared and controlled by either the customer or the expert without the latency, complexity, or cost of third-party conferencing or collaboration tools.

For more information about Direct Connect, please see the [Cisco Remote Expert Manager 1.8 Installation Guide](#).

## 3.3 Customer Location

A typical Cisco Remote Expert Smart Solution deployment may include the following components at the Customer Location:

- Cisco TelePresence System (CTS) 500 Series, EX60 or EX90 endpoints
- Cisco Interactive Experience Client (IEC-4600)
- Common Unix Printing System (CUPS)-compliant laser printer
- Collaboration Panel (touch-screen monitor)
- Human input devices (card readers, wet-ink signature capture, etc.)

### 3.3.1 Interactive Experience Client (IEC) 4610

The IEC4610 is a small (size of a paperback), low power, silent mini-computer. It weighs around three pounds and consumes on average 13W of power. The IEC comes with Ethernet CAT5 and VGA cables and mounting hardware.

The IEC has many interfaces and following are the list of its usages.

Figure 4: IEC Ports (rear)



Figure 5: IEC Ports (side)



USB ports - There are four USB ports on the IEC4602 to connect client-facing peripheral devices for the RE solution.

HDMI port - This port is connected to the TelePresence (TP) endpoint's PC or data calibration Video (in) port. This is used for displaying the static graphic image on the TP while the TP is not in an active call (e.g. TP video screen showing Off-hours, Working Hours, etc.)

VGA port - This port is the main display port that either connected to the ELO or 3M touchscreen's DVI/VGA port using a VGA-VGA cable (or VGA-DVI cable) directly.

Stereo jack - The audio cable (left and right) from the touchscreen monitor (customer pod) will be connected to this stereo jack. The audio part of the video streaming will be heard from these speakers.

LAN port - A 10/100 Mbps fast Ethernet port is used for network connection and it supports either DHCP based IP addressing or static IP addressing.

For more information, refer to the Cisco Interactive Experience Client 4600 Series User Guide:

[http://www.cisco.com/en/US/products/ps12435/tsd\\_products\\_support\\_maintain\\_and\\_operate.html](http://www.cisco.com/en/US/products/ps12435/tsd_products_support_maintain_and_operate.html)



## 4 Implementation Summary

---

The following chapters will guide you through the necessary steps in order to integrate the Remote Expert Smart Solution with a new or existing UC/CC infrastructure, including provisioning, installing and configuring the Remote Expert Manager and Customer Pods. The suggested order of steps is as follows:

1. Video Endpoint Provisioning
2. Unified Communications Manager Configuration
3. Unified Contact Center Enterprise Configuration
4. Computer Telephony Services Configuration
5. VXML Gateway Router Configuration
6. Customer Voice Portal Server Configuration
7. Cisco Agent Desktop Server Configuration
8. Cisco Agent Desktop Client Configuration
9. Interactive Experience Manager Installation and Configuration
10. Interactive Experience Client Provisioning and Configuration
11. Remote Expert Manager Hardware Provisioning
12. Media Server Integration
13. Remote Expert Manager Installation and Configuration
14. Direct Connect Installation, Configuration and Integration with CAD

## 5 Video Endpoint Provisioning

---

The Remote Expert Smart Solution version 1.8 supports the following video endpoint platforms at either the Customer Pod or the Agent Locations:

- Cisco TelePresence EX60 and EX90 Series
- Cisco TelePresence CTS-500 Series

This chapter provides you with the information you need to integrate video endpoints with the Remote Expert Smart Solution and includes the following sections:

- Licensing
- Firmware
- Component Checkpoint: Verify your work
- Troubleshooting

### 5.1 Licensing

Based on the platform, different feature licenses are required:

#### 5.1.1 Cisco TelePresence EX60 and EX90 Series

For procedures on obtaining and installing licenses for the TelePresence EX60 and EX90 Series endpoints, please refer to the [Cisco TelePresence System EX60 and EX90 Administrator Guide \(TE6.0\)](#).

#### 5.1.2 Cisco TelePresence CTS-500 Series

For procedures on obtaining and installing licenses for the TelePresence CTS-500 series endpoints, please refer to the [Configuring the Cisco TelePresence System](#) guide.

### 5.2 Firmware

Note: The EX60/90 must be running at least TC5.1 firmware before it can be upgraded to TE6.0 or higher.

Please refer to the [Remote Expert Smart Solution 1.8 Release Notes](#) for information on the firmware required for each platform supporting the features and functionality required for successful integration with the Remote Expert Smart Solution.

Best practice calls for insuring that all endpoints are updated to the required firmware levels and tested for basic functionality prior to proceeding with subsequent configuration of the solution. The firmware updates can be accomplished either via upgrading the endpoints as standalone devices or automatically when the devices initially register with CUCM. For platform-specific upgrade procedures, please refer to the following documents:

- EX60/90: [Cisco TelePresence System EX60 and EX90 Administrator Guide \(TE6.0\)](#)
- CTS-500: [Configuring the Cisco TelePresence System](#)

## **5.3 Component Checkpoint: Verify your work**

After completing the upgrade procedure, verify your work by carrying out the following tasks:

### **5.3.1 Verify Touchpanel Information**

Use the attached Touchpanel (or IP phone, in the case of the CTS-500 series) to verify that the endpoint is operating at the correct firmware level, and reflects all the required licensed features.

### **5.3.2 Browse to Endpoint Administration Page**

Using a web-browser, browse to the endpoint's administration page. Be sure that you can reach the administration page and log in with administrator privilege.

### **5.3.3 SSH To Endpoint Command Line Interface**

Using an ssh client, connect to the endpoint's command line interface. Be sure that you can connect via SSH and log in with administrator privilege.

## 6 Unified Communication Manager Configuration for Remote Expert

---

### 6.1 General CUCM Configuration

In this section we will go over the Cisco Unified Communication Manager 9.0 specific configuration information required for proper integration into the Remote Expert solution. This is more likely to be based off the Cisco Unified Communications platform best configurations of the likes of a Cisco Unified product SRND, though there might be various means to achieve the same results.

#### 6.1.1 Audio Codec Preference List

The Remote Expert 1.8 System supports G.711 as the default audio codec and H264 as the default video codec. With CUCM 9.0, Cisco has introduced a new feature called audio codec preference list. Using this, you can create a preference list with the audio codec of preference (g711 in our case) ordered on top of the list and then associate this list to a specific region. The audio codec preference list can be applied to calls both within the region and between regions.

With the Audio Codec Preference feature, you can:

- Change the relative priorities of audio codecs.
- Save the custom Audio Codec Preference list with a unique name.
- Assign custom codec preference lists for use within a region or between regions.
- Create multiple custom codec preference list.

Steps:

1. Login to CUCM as administrator user.
2. Proceed to **System > Region Information > Audio Codec Preference**
3. Click on Add New option
4. Select one of the pre-existing options from the drop down. (Options are Factory Default low loss, Factory default lossy)
5. Click on Copy
6. Give the list a new name, for instance RE18\_G711\_G722
7. Move up G711 U-law 64k and G711 A-law 64k up the list of codecs.
8. Move up the other 2 G711 codecs up the list.
9. Next move the G722 codec variations up the list, but below the G711 codecs.
10. Save.

Now, create a region called RE-Region, select this region and click on modify if required. Once in the region configuration page, select the newly created audio codec preference list for within the region in the RE 1.8 use case. Also create a standard device pool called RE-Device Pool and associate the RE-Region to the RE-Device Pool.

## 6.1.2 SIP Trunk configuration

There are 2 SIP trunks that need to be added to CUCM for this solution: one pointing to the CVP for handling the Contact Center Routing and VXMLGW interactions and another optional SIP trunk to CUBE for forking to MediaSense, for recording purposes. If you have a Highly Available setup with 2 CVP's and 2 CUBE's, then consider trunking to each of these nodes. In terms of configuration, the default configuration that CUCM offers while adding a new SIP trunk should be good for both cases.

Figure 6: Sample SIP Trunk configuration

The screenshot displays the 'Trunk Configuration' page in the Cisco Unified CM Administration console. The page is titled 'Cisco Unified CM Administration' and includes a navigation menu at the top with options like System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, and Help. Below the navigation menu, there are buttons for Save, Delete, Reset, and Add New. The main configuration area is divided into several sections:

- Status:** Status: Ready
- Device Information:**
  - Product: SIP Trunk
  - Device Protocol: SIP
  - Trunk Service Type: None(Default)
  - Device Name\*: CUBE\_SIP\_Trunk
  - Description: CUBE SIP Trunk
  - Device Pool\*: RE-DevicePool
  - Common Device Configuration: < None >
  - Call Classification\*: Use System Default
  - Media Resource Group List: RE-MRGL
  - Location\*: Hub\_None
  - AAR Group: < None >
  - Tunneled Protocol\*: None
  - QSIG Variant\*: No Changes
  - ASN.1 ROSE OID Encoding\*: No Changes
  - Packet Capture Mode\*: None
  - Packet Capture Duration: 0
  - ☐ Media Termination Point Required
  - ☒ Retry Video Call as Audio
  - ☐ Path Replacement Support
  - ☐ Transmit UTF-8 for Calling Party Name
  - ☐ Transmit UTF-8 Names in QSIG APDU
  - ☐ Unattended Port
  - ☐ SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
  - Consider Traffic on This Trunk Secure\*: When using both SRTP and TLS
  - Route Class Signaling Enabled\*: Default
  - Use Trusted Relay Point\*: Default
  - ☒ PSTN Access
  - ☐ Run On All Active Unified CM Nodes
- Intercompany Media Engine (IME):** E.164 Transformation Profile: < None >
- Multilevel Precedence and Preemption (MLPP) Information:** MLPP Domain: < None >
- Call Routing Information:**
  - ☒ Remote-Party-Id
  - ☒ Asserted-Identity
  - Asserted-Type\*: Default

SIP Privacy\* Default

---

**Inbound Calls**

Significant Digits\* All

Connected Line ID Presentation\* Default

Connected Name Presentation\* Default

Calling Search Space < None >

AAR Calling Search Space < None >

Prefix DN

☐ Redirecting Diversion Header Delivery - Inbound

---

**Incoming Calling Party Settings**

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

Clear Prefix Settings Default Prefix Settings

Number Type	Prefix	Strip Digits	Calling Search Space	Use Device Pool CSS
Incoming Number	<span>Default</span>	<span>0</span>	<span>&lt; None &gt;</span>	<input checked="" type="checkbox"/>

---

**Connected Party Settings**

Connected Party Transformation CSS < None >

☒ Use Device Pool Connected Party Transformation CSS

---

**Outbound Calls**

Called Party Transformation CSS < None >

☒ Use Device Pool Called Party Transformation CSS

Calling Party Transformation CSS < None >

☒ Use Device Pool Calling Party Transformation CSS

Calling Party Selection\* Originator

Calling Line ID Presentation\* Default

Calling Name Presentation\* Default

Calling and Connected Party Info Format\* Deliver DN only in connected party

☐ Redirecting Diversion Header Delivery - Outbound

Redirecting Party Transformation CSS < None >

☒ Use Device Pool Redirecting Party Transformation CSS

---

**Caller Information**

Caller ID DN

Caller Name

☐ Maintain Original Caller ID DN and Caller Name in Identity Headers

---

**SIP Information**

---

**Destination**

☐ Destination Address is an SRV

1\* Destination Address 192.168.71.56 Destination Address IPv6 Destination Port 5060 + -

MTP Preferred Originating Codec\* 711ulaw

BLF Presence Group\* Standard Presence group

SIP Trunk Security Profile\* Non Secure SIP Trunk Profile

Rerouting Calling Search Space < None >

Out-Of-Dialog Refer Calling Search Space < None >

SUBSCRIBE Calling Search Space < None >

SIP Profile\* Standard SIP Profile

DTMF Signaling Method\* No Preference

---

**Normalization Script**

Normalization Script < None >

☐ Enable Trace

	Parameter Name	Parameter Value
1		

---

**Geolocation Configuration**

Geolocation < None >

Geolocation Filter < None >

☐ Send Geolocation Information

---

Save Delete Reset Add New

---

**Legend:**

- \* - indicates required item.
- \*\* - Device reset is not required for changes to Packet Capture Mode and Packet Capture Duration.

**Note** Ensure that the Media Resource Group List added for this RE solution (RE-MRGL) is selected as the MRGL on the SIP trunk pointing to the CUBE, since the videoconference bridge will be a call leg on the CUBE in Video Conference use cases.

### 6.1.3 Route Pattern configuration

Once the SIP trunk has been configured to CVP, create a route pattern in CUCM and associate this pattern to the SIP trunk pointing to CVP.

#### Steps

1. Login to CUCM as Administrator user
2. Proceed to Call Routing -> Route/Hunt -> Route Pattern
3. Click Add New
4. Set the Route Pattern to the Pilot point DN that is sent to UCCE.
5. Set the Gateway/Route List to the SIP trunk created to point to CVP.
6. Set Route option to "Route this pattern"

Figure 7: Sample Route Pattern Configuration

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾

**Route Pattern Configuration**

Save

**Status**

Status: Ready

**Pattern Definition**

Route Pattern\*

Route Partition

Description

Numbering Plan

Route Filter

MLPP Precedence\*

☐ Apply Call Blocking Percentage

Resource Priority Namespace Network Domain

Route Class\*

Gateway/Route List\*  [\(Edit\)](#)

Route Option  
☒ Route this pattern  
☐ Block this pattern

Call Classification\*

☐ Allow Device Override ☒ Provide Outside Dial Tone ☐ Allow Overlap Sending ☐ Urgent Priority

☐ Require Forced Authorization Code

Authorization Level\*

☐ Require Client Matter Code

### 6.1.4 Disable Music On Hold (MOH)

There are use cases in the Remote Expert Smart Solution/System where the MOH played from the CUCM MOH might conflict with the audio of the video pushed by REM's media server. In order that the

REM played audio/video might take priority over the CUCM MOH, we disable the MOH on the CUCM for the devices that are placed at the Customer pods/Kiosks.

### Steps

1. Login to CUCM as Administrator user
2. Proceed to Media Resources -> Fixed MOH Audio Source
3. Specify a Name and tick the enabled check box.
4. Click on Save
5. Apply this MOH to the *User Hold MOH Audio Source* and *Network Hold MOH Audio Source* fields on the configuration page of the end points, which are placed at the expert end.

Figure 8:Fixed MOH Audio Source Configuration

**Fixed MOH Audio Source Configuration**

Save Delete

**Status**  
Status: Ready

**Fixed MOH Audio Source Information**  
Source ID\* 51  
Name\* Silence  
☐ Allow Multi-casting  
☒ Enable (If checked, Name is required.)

**Announcement Settings**  
Initial Announcement -- Not Selected -- View Details  
Initial Announcement Played\* Always  
Periodic Announcement -- Not Selected -- View Details  
Periodic Announcement Interval\* 30 (10 - 300 seconds)  
Locale Announcement\* English United States

Save Delete

\*- indicates required item.

Figure 9:Device Configuration

User Hold MOH Audio Source	51-Silence
Network Hold MOH Audio Source	51-Silence

### 6.1.5 Conference Bridge

**Note:** This is an optional feature for the Remote Expert Smart Solution roll out and only needs to be configured if Video Conferencing from an expert station becomes a requirement for the deployment.

Remote Expert solution requires a videoconference bridge to be registered to CUCM to facilitate videoconference use cases where a customer at a Remote Expert Customer Pod / Kiosk is connected to Expert1 and Expert1 conferences in Expert2 for further assistance.



**Steps:**

1. Login to CUCM as administrator user.
2. Proceed to **Media Resources -> Conference Bridge**
3. Click on Add New
4. Select Cisco Telepresence MCU as the Conference Bridge Type under Hardware Conference Bridge Info.
5. Configure the Conference Bridge name (user defined) and the destination IP address (IP address of the MCU)
6. Select the device pool to which the Remote Expert Customer endpoints are allocated as the Device Pool of the MCU.
7. Under the SIP interface info, enter 5060 (default) for the MCU Conference Bridge SIP port.
8. Select the default Non Secure Sip Trunk Profile as the SIP trunk security profile and Standard SIP profile as the SIP profile for the MCU.
9. Under HTTP interface info, provide the MCU GUI login details like User name and password. Also provide 80 as the HTTP port.

Once this is done, add an MRG (RE-MRG) in CUCM and select this conference bridge to be part of the MRG. Add this MRG to an MRGL (RE-MRGL) use this MRGL in other CUCM configurations like SIP Trunks and Device pools.

**Note** Before you add the MCU to the CUCM, ensure the Codian MCU is configured and the CUCM is added to the MCU settings. Refer to section 22.1 for MCU configuration details.

## 6.2 Device Specific Configuration

### 6.2.1 Cisco TelePresence System (CTS) Endpoints

For detailed instructions on setting up and registering the Cisco TelePresence System endpoint to the Cisco Unified Communications Manager, read the [Configuring the Cisco TelePresence System](#) section of the Cisco TelePresence System Admin Guide.

Once the CTS endpoint is registered to Cisco Unified Communications Manager, the following checklist will help do a quick verification if the device is setup correctly for Remote Expert:

1. Ensure that the correct version of software is loaded on the EX endpoints. Confirm with section 5.2
2. CTS endpoint is allocated a valid DN in the Customer/Kiosk DN range or the Expert endpoint DN range based on where it is being set up.
3. On the phone configuration page select the correct device pool created for Remote Expert.
4. On the endpoints placed at Customer stations/Kiosks, disable the MoH audio.

## 6.2.2 EX Endpoints

For detailed instructions on setting up and registering an EX endpoint to Cisco Unified Communications Manager, please refer to the [EX Series Administrator Guide](#) available on Cisco.com.

Steps:

1. Power up the EX endpoint
2. EX will go through its boot up cycle and eventually provide a configurable screen. Ensure the endpoint has obtained an IP address either by DHCP or manual configuration method.
3. Proceed to the endpoints web interface [http://ex\\_ipAddress](http://ex_ipAddress)
4. Login using admin/admin as the default credentials.
5. Proceed to Configuration -> Advanced Configuration
6. Select Provisioning Menu from the left panel
7. On the right, set Mode to CUCM and set External Manager Address to the CUCM IP Address, with protocol set to http. Leave the rest of the configurations at its defaults.

This should register the endpoint to the CUCM, provided auto registration is turned on at the CUCM administration. If not, manually add this EX endpoint to CUCM before attempting the steps mentioned above.

If you are facing issues with registering the EX endpoint to CUCM, refer to [TE6.0 Release Notes](#) & [Troubleshooting guides](#) for help.

Once the EX endpoint is registered to Cisco Unified Communications Manager, the following checklist will help do a quick verification if the device is setup correctly for Remote Expert:

1. Ensure that the correct version of software is loaded on the EX endpoints. Confirm with section 5.2
2. EX is allocated a valid DN in the Customer/Kiosk DN range or the Expert endpoint DN range based on where it is being set up
3. On the phone configuration page select the correct device pool created for Remote Expert
4. On the EX endpoints placed at Customer stations/Kiosks, disable the MoH audio

## 6.3 CTI Specific Configuration

### 6.3.1 Application User Accounts

#### 6.3.1.1 JTAPI Application User configuration to talk to REM

The Remote Expert Manager (REM) talks to Cisco Unified Communication Manager using CUCM JTAPI interface. On the CUCM, a JTAPI/application user is configured for this purpose, which will later be referenced during initial REM setup and configuration by pointing to it in the “REM.properties” file under the CUCM Credentials section.

Steps:

1. Login to CUCM as an admin user
2. Proceed to Users Management -> Application User

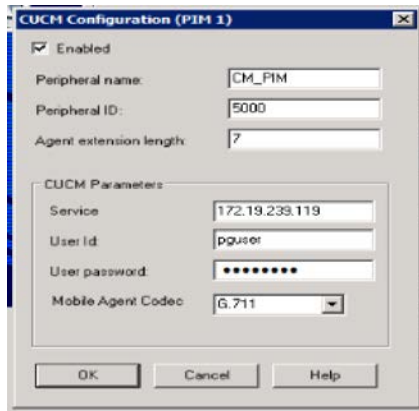
3. Click on Add New user and the New Application User Configuration page is loaded.
4. Provide the application user a suitable User ID and password.
5. Next move to the Device Information section.
6. Select the CTS/EX endpoints that will be monitored by REM from the Available Devices list. In our case it will be all of the endpoints that will be placed in both customer pod and Expert locations.
7. Move the devices selected in step 6 to the controlled devices list below.
8. Proceed to the Permissions Information section
9. Click on Add to Access Control Group button
10. A popup is rendered with Find Access Control Groups page.
11. Select Standard CTI Enabled, Standard CTI Allow Control of All Devices, Standard CTI Allow Control of Phones supporting Conference from this list and click OK. The corresponding Roles get automatically selected.
12. Now click on save button.

Figure 10: Sample JTAPI application user configuration

### 6.3.1.2 JTAPI Application User configuration to talk to UCCE/PG

Just as with REM, the Agent Peripheral Gateway (PG) in the Unified Contact Center Enterprise (UCCE) framework talks to CUCM using the JTAPI interface. The configuration of a JTAPI application user is the same as explained in section 6.3.1.1 above. This user is input into the Call Manager PIM configuration of the Agent PG setup. This configuration is explained in Chapter 7.

Figure 11: Sample CUCM JTAPI user in Agent PG configuration



**Note** When selecting the CTS devices, make sure to separate the 7970 phone and the CTS Codec since they are configured as shared lines in CUCM and UCCE does not support shared line on CUCM PIM. This would not allow the call to be properly routed to the expert (CTS).

### 6.3.2 End User Accounts

In the Remote Expert solution we have two end users configured in CUCM. One would be the administrator user for CUCM administration and this user would be created during the CUCM installation phase.

There is a need for an AXL end user configuration on CUCM to talk to the MediaSense recording server which is optional based on customer requirement to either support audio recording or not. This user

would be also configured in the Unified CM Configuration page of the MediaSense Admin interface. The screenshots for both are pasted below.

Figure 12: Sample AXL user on CUCM to talk to MediaSense

The screenshot displays the Cisco Unified CM Administration web interface. The top navigation bar includes links for System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The main heading is 'End User Configuration'. Below this, there are buttons for Save, Delete, and Add New, along with a status message 'Add successful'. The 'User Information' section is expanded, showing fields for User Status (Active Local User), User ID\* (msapi), Password, Confirm Password, PIN, Confirm PIN, Last name\* (MediaSense), Middle name, First name, Directory URI, Telephone Number, Mail ID, Manager User ID, Department, User Locale (set to < None >), Associated PC, Digest Credentials, Confirm Digest Credentials, Name Dialing (MediaSense), and Number of Digits needed for the Unique AA Name (1). There are 'Edit Credential' buttons next to the Password and PIN fields.

Figure 13: Sample MediaSense AXL Provider Configuration

The screenshot shows the 'Unified CM Configuration' web interface. At the top, there are buttons for 'Save', 'Reset', and 'Modify Unified CM Cluster'. Below these, a green checkmark icon is followed by the message: 'The AXL Service Provider credentials are incorrect. Verify your ip address, username, and password and re-submit.' The main section is titled 'AXL Service Provider Configuration'. It contains two side-by-side lists: 'Available AXL Service Providers' (which is currently empty) and 'Selected AXL Service Providers' (which contains the IP address '172.19.239.119'). Between these lists are two small orange arrow buttons for moving items. At the bottom, there are input fields for 'Username' (containing 'msapi') and 'Password' (containing a masked password '\*\*\*\*\*').

## 6.4 Component Checkpoint: Verify your work

### 6.4.1 Make video calls

At this point, the only real test to verify your configuration would be to make video calls between endpoints (Customer and Expert) registered to the CUCM.

## 6.5 Troubleshooting

- EX Series Won't Register: Verify DNS domain name
- EX won't register: Check if the endpoint has a release key installed.
- CTS won't register: Confirm that the 7970 associated with the CTS, and the CTS video unit, share a single line.

## 7 Unified Contact Center Enterprise (UCCE) Configuration Specifics for Remote Expert

---

### 7.1 UCCE Installation Pre-requisites

This section has been put together by consolidating information from various UCCE Installation/Administration guides. The full installation and design guidance for the Cisco Unified Contact Center Enterprise can be found in the [Cisco Unified Contact Center Enterprise Solution Reference Network Design \(SRND\)](#).

The system prerequisites are also covered in the [Staging Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted](#). The staging guide covers all information pertaining to OS installation, SQL server installation & configuration, system tweaks and registry modification (if any). It should be sufficient to follow these guidelines to setup the UCCE base nodes. In this document, we assume that the OS is correctly installed & setup and system pre-requisites such as SQL Server 2008 R2 have been installed in the right order, patches have been applied to the operating system etc.

#### 7.1.1 ICM Setup Program

The ICM Setup program allows you install, update, and configure your ICM software. It is located on the ICM CD. Run Setup on each machine in the ICM system: each Call Router, each Logger, each Peripheral Gateway (PG), and each Admin Workstation. At the initial installation, a local version of the Setup program is installed on each ICM component at `\icm\bin\ICMSetup.exe`. (On an Admin Workstation, the Cisco Admin Workstation group contains an icon for this program.)

In order to run Setup, you must be a local administrator and belong to the setup group for any instance that you are installing a component.

**Note** During the installation of the Central Controller and Administration and Web View Reporting, the ICM installer checks to see whether there is a Microsoft.NET Framework 3.5 installed. If it is not installed, Setup will install it. After the installation of the Microsoft.NET Framework 3.5, it might prompt you to reboot the system. If prompted, reboot the system and run Setup again.

#### 7.1.2 Creating an ICM Instance

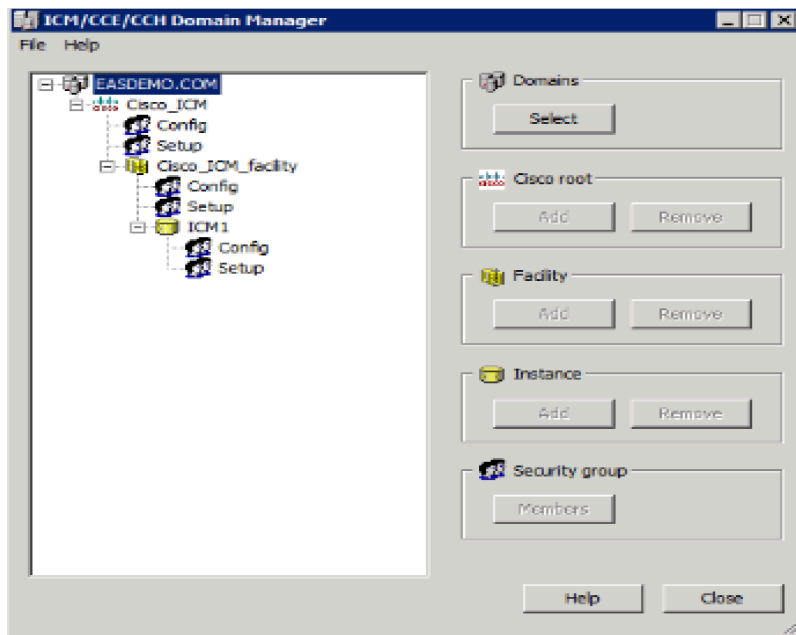
- Before any ICM components can be installed an ICM instance must first be created
- Before an instance can be selected the proper entries must first be created in the domain using the Domain Manager

#### 7.1.3 Configure Domain Manager

Steps:

1. Start the Cisco Unified ICM installation by running the ICMSetup.exe application on the CD or local directory as appropriate.
2. Click the Domain Manager.
3. Select the desired domain from the list on the left and click ADD, then click OK.

4. After the domain is selected, click Add it under the Cisco root section. Enter an appropriate name such as Cisco\_ICM and click OK.
5. With the new root selected, click the ADD button under the Facility option. Enter an appropriate Facility name such as Cisco\_ICM\_Facility and click OK.
6. Once the Facility has been added, select it and click Add under the Instance option. Enter an instance name such as ICM and click OK.
7. After adding the root, facility and instances click close. After the domain components have been created, you can then add the instance in the ICM setup.
8. At least one ICM instance must be added before you can install any ICM components. Before you can create an ICM instance, you must have set up the Windows Active Directory services for ICM software. You must also have added the Cisco Root Organizational Unit, and at least one Facility Organizational Unit with one Instance Organizational Unit.
9. In the Cisco ICM Setup dialog box, in the ICM Instances section, click Add. The Add Instance dialog box opens:
  - a) Select the network Domain for the instance.
  - b) Select the Facility Organizational Unit for the instance.
  - c) Select the Instance Name for the instance.



Use the **Instance Number** generated by the ICM software. (For standard single-instance ICM configurations, the instance number is 0.)

**Note** The mappings of instance names to instance numbers must be the same on every node in the system.



## 7.2 UCCE Components

### 7.2.1 Router Installation

Steps:

1. In the ICM Setup application, click the Add button on the right under Instance Components. A new dialogue window will appear where you will be able to select the Router component.
2. For high availability installations select the Duplexed Router option and click next.
3. Click next.
4. The number of PGs must be entered as a range or comma separated list. For the two PGs, it could be entered as either "1-2" or "1,2". (One for CUCM and another as VRU PG for CVP)
5. Accept the current settings and click on next for the following screens.
6. It is best practice to use IP addresses rather the hostnames when identifying the public and private
7. If the Call Router is simplexed, enter localhost in both the B and B high fields.
8. After entering the Router interface IP addresses click next.
9. At the ICM setup, review the installation settings and click next to complete the installation of the Call Router.

### 7.3 Logger Installation

In the ICM Setup application, click the Add button on the right under "Instance Components". A new dialogue window appears where you will be able to select the Logger component.

Steps:

1. Select production, Auto startup (and Duplexed logger in case of a HA build out) options, and then click Next.
2. Configure the public and private Router and Logger interfaces using the IP address. Click Next.
3. At the end of the ICM setup, review the installation settings and click Next to complete the installation of the Call Logger.

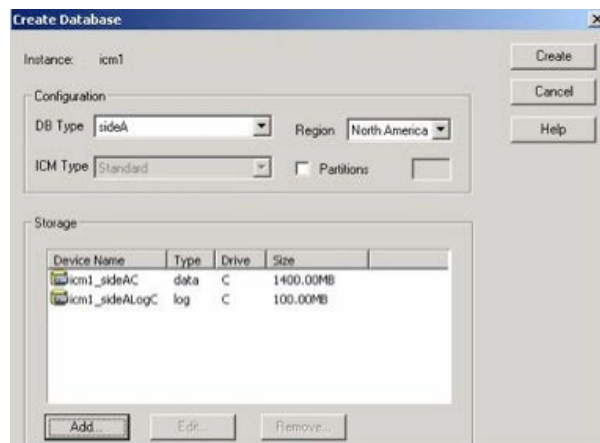
#### 7.3.1 Logger Configuration

You must create a database for each Logger; it is best to do this before installing other components. To create the database and determine the appropriate size of the database, run the ICM Database Administration (ICMDBA) tool. This tool is installed on each ICM component that has an installed database (ICMDBA is in the \icm\bin directory) and on each Admin Workstation.

Once the proper size is determined, run the icmdba.exe file from the local ICM directory to create and configure the new database.

If you are prompted that the SQL Server is not configured properly, click yes and then set the memory requirement to 0 and the recovery interval to 1. As this may have interrupted the installation process, you will see that no new database has been created. You need to once again select "Create" under the database option.

This time all the necessary changes have been made, you will be able to create the database. Now add the data and log databases to the list and create the database.



Once the database is created successfully click OK.

### 7.3.2 Admin Workstation (AW) Installation

After completing the installation of the Router and Logger, the Admin Workstation can be set up. The Admin workstation is configured before the other PGs as it assigns the IDs needed for the Router, Logger, and PGs to communicate through.

The Admin Workstation (AW) serves as a control console where you can monitor agent and contact center activity and change how the ICM software routes contacts. For example, you can use the Admin Workstation to configure the ICM contact center data and to create routing scripts. Admin Workstations can be located anywhere, as long as they have LAN, WAN, or dial-up connections to the ICM software. Typically, the Admin Workstation is installed on a Windows operations console used by system administrators, not the Router, Logger, or other ICM server systems. It requires an SQL database and must be a member of the Active Directory Domain.

Steps:

1. From the ICM Setup applications, select Add for the ICM instance and then "Admin Workstation".
2. Select Real-Time Distributor under Admin Workstation Configuration, Standard for AW Type and enable Production Mode. Click Next.
3. Select Auto Start at System Startup under Node Manager Properties, enable Internet Script Editor and Do not modify service accounts under Service Account Management. Click Next.
4. Enter an admin site name. Select Central Controller Side A Select Next.
5. Verify Setup parameters and select Next to finish.

After the AW installation is complete, you must initialize the local database. The initialize database dialogue will appear after the Admin Workstation module installation is completed.

When you install a Distributor Admin Workstation, ICM Setup automatically sizes and creates a local database on the machine. Because this database is constantly overwritten by new data, the database

size remains fairly constant. You normally do not need to resize the Distributor Admin Workstation (AW) real-time database. If you do need to resize the Distributor AW database, you can do so using the ICM Database Administration (ICMDBA) tool.

### 7.3.3 Admin Workstation (AW) Configuration

Each peripheral communicates with ICM software through a Peripheral Gateway, called a PG. The PG is a computer that communicates directly with the ACD, PBX, VRU, or Call Manager at a contact center, monitoring status information from the peripheral and sending it to the ICM system's Central Controller. If the peripheral acts as a routing client, the PG sends routing requests to ICM software.

The PG can be a single-simplex computer or a pair of duplexed computers. A single PG can service more than one peripheral; however, each peripheral uses only one PG.

Before adding the peripheral gateways to the CUCCE Servers, they must first be created in the Admin Workstation Configuration Manager. This generates the peripheral IDs that are necessary for the PG/PIM installations.

To create the peripheral gateways in Configuration Manager there must first be an Agent Desk Settings List entry as it is one of the required settings under a PG controller configuration.

In the following sections we will take a look at some basic configurations in the Admin Workstation Configuration Manager that are required for Contact Center setup in Remote Expert.

#### 7.3.3.1 *Agent Desk Settings*

1. Open the Configurations Manager on the AW.
2. Select the Agent Desk Settings List option under the Tools >Explorer Tools group.
3. Click Retrieve.
4. Click Add.
5. Enter an appropriate list name such as Agent\_Desk\_Settings\_1.
6. Enter a proper description.
7. Set the Ring no Answer time to 60.
8. Set the Wrap up time to 20.
9. Click Save.

The 'Attributes' window shows configuration for 'Agent\_desk\_settings\_1'. Fields include: Name (Agent\_desk\_settings\_1), Ring no answer time (10 seconds), Ring no answer dialed number (<None>), Logout non-activity time (seconds), Work mode on incoming (Optional), Work mode on outgoing (Optional), Wrap up time (20 seconds), Assist call method (Consult), Emergency alert method (Consult), and Description. There are two sections of checkboxes: 'Miscellaneous' (Auto answer, Idle reason required, Logout reason required, Auto record on emergency) and 'Outbound Access' (International, National, Local private network, Operator assisted, PBX). At the bottom, there is an 'Enable Cisco Unified Mobile Agent' checkbox and a 'Mobile agent mode' dropdown set to 'Agent chooses'.

To create the peripheral gateways in Configuration Manager, there must also be a Media Routing Domain list entry as it is one of the required settings under a PG controller configuration.

#### 7.3.3.2 Media Routing Domain

1. Open the Configurations Manager on the AW.
2. Select the Media Routing Domain List option under the Tools > Explorer Tools group.
3. Click Retrieve.
4. Click Add.
5. Enter an appropriate list name such as Cisco\_Voice.
6. Enter a proper description.
7. Set the Media Class to Cisco\_Voice.
8. Click Save

The 'Media Routing Domain List' window shows a list of domains on the left with 'Cisco\_Voice' selected. The right pane shows the 'Attributes' for this domain. Fields include: Name (Cisco\_Voice), Media routing domain ID (1), and Media class (Cisco\_Voice). There is a table for 'Task' settings with columns for 'Task' and 'Override Media Class Default'. The tasks listed are Life, Start timeout, and Max duration, all with values of 0 seconds. Below this is a 'Calls in Queue' section with fields for Max, Max per call type, and Max time in queue. The 'Service level threshold' is set to 10, and the 'Service level type' is 'Ignore Abandoned Calls'. There is an 'Interlocute' checkbox and a 'Description' field with the text 'Default Media Routing Domain for Cisco\_Voice'.

Once the Agent Desk setting list and the Media Routing Domain have been created, the new PG logical controllers for the Call Manager and CVP can be created.

There are several methods for creating PGs and their underlying Peripheral Interface Managers (PIMS). For this solution, only 1 PG is created. It is a Generic PG and has the CUCM and VRU\_CVP PIMS. The PG Explorer on the AW Configuration Manager generates and maintains PG records for a logical interface controller, a physical interface controller, associated peripherals, and, if appropriate, an associated routing client.

### 7.3.3.3 *Peripheral gateway logical controller*

1. Open the Configurations Manager on the AW.
2. Select the PG Explorer option under the Tools > Explorer Tools group.
3. Click Retrieve.
4. Click Add PG.
5. Enter an appropriate name such as Generic\_PG\_1.
6. Enter a proper description.
7. Set the client type to PG Generic.
8. Set the IP address for the CTI Server.
9. Click Save.

After clicking save, the logical and physical controller IDs will be automatically generated. Note them for later use when installing the peripheral gateways in ICMSetup later.

After creating the logical controller, the first of the underlying peripherals can now be added as follows:

1. Select the Generic\_PG\_1 PG that was just added from the PG explorer results on the left.
2. Click Add Peripheral.
3. Enter an appropriate peripheral name such as CCM\_PIM.
4. Select the Client Type as Call Manager/SoftACD.
5. Select the Default Desk Settings option that was created earlier Agent\_Desk\_Settings\_1.
6. Enter a proper description.
7. Check the Enable post routing option.

## 8. Then Click Save.

After clicking Save the peripheral ID will be automatically generated; note it for later use when installing the peripheral gateways in ICM Setup.

Skill Group Mask	Routing client	Default route	Peripheral Monitor
Peripheral	Advanced	Agent Distribution	
Peripheral ID:	* 5000		
Name:	* CM_PIM		
Peripheral name:	* CM_PIM		
Client type	* CUCM/SoftACD		
Location:			
Abandoned call wait time:	* 5		
Configuration parameters:			
Call control variable map:			
Default desk settings:	Agent_desk_settings_1		
Peripheral service level type:	* Calculated by Call Center		
Agent Phone Line Control:	* All Lines		
Non ACD Line Impact:	* Available Agent Stays Available		
Description:			
Enable post routing:	<input checked="" type="checkbox"/> Peripheral auto configured: <input type="checkbox"/>		

Select the Routing Client tab and enter the following information for the peripheral:

1. Enter an appropriate name and Peripheral name such as CUCM\_RC.
2. Select the Client Type as PCC/Enterprise Agent.
3. Select the Default media routing domain option to Cisco\_Voice.
4. Enter a proper description.
5. Click Save.

Peripheral	Advanced	Agent Distribution
Skill Group Mask	Routing client	Default route
Name:	* CM_RC	ID: * 5000
Timeout threshold:	* 1500	
Late threshold:	* 500	
Timeout limit:	* 10	
Default media routing domain:	Cisco_Voice	
Default call type:	NONE	
Configuration parameters:		
Dialed Number/Label map:	* Do not use DN/Label map	
Client type:	* IPCC / Enterprise Agent	
Description:		
Network routing client:		
Network transfer preferred:	<input checked="" type="checkbox"/>	
Congestion Treatment Mode:	Treat call with Global Default Label	
Default Label:		

6. On the Default Route tab ensure that Cisco\_Voice is selected.

Media routing domain	Route
Cisco_Voice	

New Delete

Media routing domain: \* Cisco\_Voice

Route: NONE

After the creation of the CUCM peripheral the second CVP VRU peripheral can now be added as follows:

1. Select the Generic\_PG\_1 PG that was added from the PG explorer results on the left.
2. Click Add Peripheral.
3. Enter an appropriate name and peripheral name such as VRU\_PIM.
4. Select the Client Type as VRU.
5. Select the Default Desk Settings option to NONE.
6. Enter a proper description.
7. Check the Enable post routing option.
8. Click Save.

After clicking Save, the peripheral ID will be automatically generated; note it for later use when installing the peripheral gateways in ICMSetup.

Peripheral ID: \* 5001

Name: \* VRU\_PIM

Peripheral name: \* VRU\_PIM

Client type: \* VRU

Location:

Abandoned call wait time: \* 0

Configuration parameters:

Call control variable map:

Default desk settings: NONE

Peripheral service level type: \* Calculated by Call Center

Agent Phone Line Control: \* Single Line

Non ACD Line Impact: \* Available Agent Stays Available

Description:

Enable post routing: ☒ Peripheral auto configured: ☐

Select the Routing Client tab and enter the following information for the peripheral:

1. Enter an appropriate name and Peripheral name such as VRU\_RC.

2. Select the Client Type as VRU.
3. Select the Default media routing domain option to Cisco\_Voice.
4. Enter a proper description.
5. Click Save.

Peripheral	Advanced	Agent Distribution
Skill Group Mask	Routing client	Default route
		Peripheral Monitor
Name:	* VRU_RC	ID: * 5001
Timeout threshold:	* 2000	
Late threshold:	* 1000	
Timeout limit:	* 10	
Default media routing domain:	Cisco_Voice	
Default call type:	call_type_1	
Configuration parameters:		
Dialed Number/Label map:	* Do not use DN/Label map	
Client type:	* VRU	
Description:		
Network routing client:		
Network transfer preferred:	<input checked="" type="checkbox"/>	
Congestion Treatment Mode:	Treat call with Global Default Label	
Default Label:		

Once all of the peripheral gateways and peripheral interface managers have been created in the Admin Workstation Configuration Manager the Peripheral Gateway (PG) can then be installed in the ICM servers.

#### 7.3.3.4 Network VRU Configuration

##### Steps

1. Open the Configurations Manager on the AW.
2. Select the Network VRU Explorer option under the Tools > Explorer Tools group.
3. Click Retrieve.
4. Click Add Network VRU.
5. Enter an appropriate name such as "cvp".
6. Select the type as "Type 10".
7. Enter a description such as the extension numbers associated with CVP and the VXML Gateway.
8. Then Click Save.

Perform the same steps and add a label for the CVP VRU PIM Route client as follows:

1. Click Add Label.
2. Select the Network VRU cvp.
3. Select the Route Client CVP\_VRU\_PIM.
4. Enter the label being returned to CVP.



5. Select normal for the label type.
6. Select icm as the Customer.
7. Enter a description as desired.
8. Click Save.

After the network VRUs have been created, add a Contact Center Agent and Skill Group for testing purposes.

#### 7.3.3.5 Add Agents

Create Agents as follows:

1. Open the Configurations Manager on the AW.
2. Select the Agent Explorer option under the Tools > Explorer Tools group.
3. Click Retrieve.
4. Click Add Agent.
5. Enter an appropriate first, last, and login name.
6. Enter an appropriate password.
7. Verify the Enterprise name that was generated is appropriate.
8. Enter an Agent ID number or allow one to be generated automatically. This number is used during agent login to the Agent desktop client.
9. On the Supervisor tab, check Supervisor agent if desired.
10. Click Save.
11. Repeat above steps to add all the agents.

#### 7.3.3.6 Add Skill Group

Create a Skill Group as follows:

1. Open the Configurations Manager on the AW.
2. Select the Skill Group Explorer option under the Tools > Explorer Tools group.
3. Click Retrieve.
4. Click Add Skill Group.

5. Enter a Peripheral name such as PreSale.
6. Enter an appropriate Name such as Generic\_Presale.
7. Select the Media Routing domain Cisco\_Voice.
8. On the Skill Group Members tab click add and select the agent created earlier.
9. Click Save.
10. Add route option in the skill group.
11. Click Add Route.
12. Assign an appropriate name such as Generic\_PreSale\_Route.
13. Click Save.

The next step is to create Call Type Lists.

#### **7.3.3.7 Add Call Type List**

Create a Call Type List as follows:

1. Open the Configurations Manager on the AW.
2. Select the Call Type List option under the Tools > Explorer Tools group.
3. Click Retrieve.
4. Click Add.
5. Enter a name such as call\_type\_1
6. Select the Customer icm.
7. Enter an appropriate description as desired.
8. Click Save.

**Attributes**

Name \*

Call Type ID \*

Customer

**Service level**

Service level threshold  ☐ Override System Information Default

Service level type  ☐ Override System Information Default

Bucket intervals  ☐ Override System Information Default

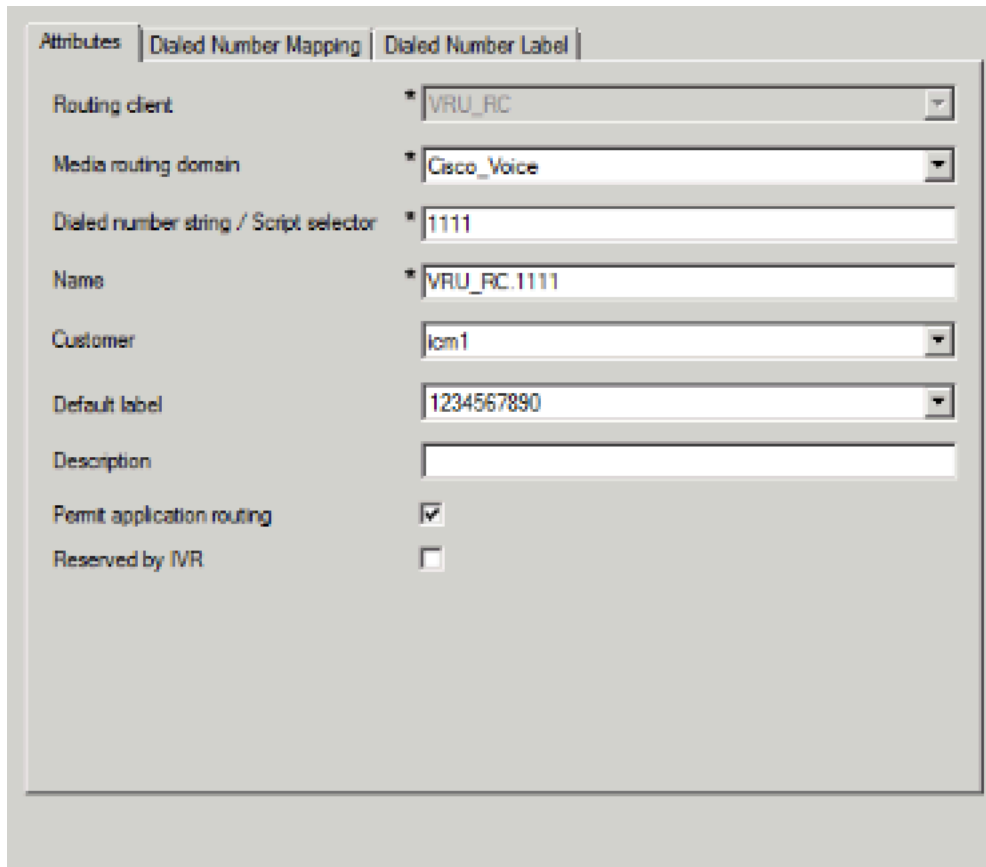
Description

#### 7.3.3.8 Add Dialed Number/Script Selector List

Create a Dialed Number List as follows:

1. Open the Configurations Manager on the AW.
2. Select the Dialed Number/ Script Selector List option under the Tools > Explorer Tools group.
3. Click Retrieve.
4. Click Add.
5. Select the Routing client CUCM\_RC.
6. Select the Media routing Domain Cisco\_Voice.
7. Enter the Dialed Number string that is called to reach this queue.
8. Enter a name such as CUCM\_RC.1000 or CUCM\_RC.1333 as appropriate.
9. Select the Customer icm.
10. Leave the default Label as <None>.
11. Enter an appropriate description as desired.
12. Click Save.
13. Repeat for additional dialed numbers.

14. On the Dialed Number Mapping Tab, select the calling line ID, Caller Entered digits (if any) and the Call type.



Field	Value
Routing client	VRU_RC
Media routing domain	Cisco_Voice
Dialed number string / Script selector	1111
Name	VRU_RC.1111
Customer	icm1
Default label	1234567890
Description	
Permit application routing	<input checked="" type="checkbox"/>
Reserved by IVR	<input type="checkbox"/>

#### 7.3.3.9 Enable Expanded Call Context

To ensure proper call routing, ensure that **Expanded call context** is enabled in the System information configuration as follows:

1. Open the Configurations Manager on the AW.
2. Select the System Information option under the Configure ICM > Enterprise > System Information group.
3. Check the Expanded call context option.
4. Click Save.

#### 7.3.3.10 ICM Instance Explorer Setting

An additional customer definition must be created for CVP under the ICM instance.

Create a customer definition as follows:

1. Open the Configurations Manager on the AW.

2. Select the ICM Instance Explorer option under the Tools > Explorer Tools group.
3. Click Retrieve.
4. Select the desired instance.
5. Click Add Customer definition.
6. Enter an appropriate name.
7. Select the Network VRU as cvp.
8. Enter an appropriate description as desired.
9. Click Save.

#### 7.3.3.11 Add Expanded Call Variable List

Call variables are used to carry various pieces of information between systems as a call flows through the queue script steps. The default installation lacks several variables used in an Expert Advisor deployment and as such need to be added.

Add additional call variables as follows:

1. Open the Configurations Manager on the AW.
2. Select the Expanded Call Variable List option under the Tools > Explorer Tools group.
3. Click Retrieve.
4. Click Add.
5. Using the table of information below, configure each variable.
6. Enter the variable name.
7. Set the variable maximum length.
8. If an array size is defined, check the array option and set the size.
9. Set the variable as enabled.
10. Set as persistent if specified.
11. Enter an appropriate description as desired.
12. Click Save.
13. Repeat for each call variable.

Expanded Call Variables				
Name	Max Length	Array size	Enabled	Persistent
user.cvpmovies_bg_media	40		yes	
user.h323.rftransfer	1		Yes	
user.media.id	36		Yes	
user.microapp.app_media_lib	10		Yes	

user.microapp.caller_input	210		Yes	
user.microapp.charset	10		Yes	Yes
user.microapp.currency	6		Yes	
user.microapp.cvpmovies_params	40		Yes	
user.microapp.error_code	2		Yes	
user.microapp.FromExtVXML	210	1	Yes	
user.microapp.grammar_choices	210		Yes	
user.microapp.inline_tts	210		Yes	
user.microapp.input_type	1		Yes	
user.microapp.locale	5		Yes	
user.microapp.media_server	30		Yes	
user.microapp.metadata	62		Yes	
user.microapp.override_cli	1		Yes	
user.microapp.pd_tts	1		Yes	
user.microapp.play_data	40		Yes	
user.microapp.recording	40		Yes	
user.microapp.sys_media_lib	10		Yes	
user.microapp.ToExtVXML	210	1	Yes	
user.microapp.uui	131		Yes	
user.microapp.UseVXMLParams	1	1	Yes	

user.sip.refertransfer	1		Yes	
user.video_media_server	40		Yes	

### 7.3.3.12 Network VRU Script List

The Network VRU enables interaction with the caller using a variety of external scripts. The scripts created in the Network VRU Script List are then made available in the Script Editor.

Create the VRU Scripts as follows:

1. Open the Configurations Manager on the AW.
2. Select the Network VRU Script List option under the Tools > Explorer Tools group.
3. Click Retrieve.
4. Click Add.
5. Create a network VRU Script for playing silence while Customer is in Video Queue.
6. Enter the script name.
7. Set the Network VRU as cvp for all entries.
8. Enter the VRU script name.
9. Enter the Timeout length.
10. Enter the Configuration parameter.
11. Set the Customer as icm.
12. Enter an appropriate description as desired.
13. Click Save.

### 7.3.3.13 Reroute on No Answer (RONA) configuration

When a call is routed to an agent but the agent fails to answer the call within a configurable amount of time, the Cisco Call Manager PIM for the agent who did not answer will change that agent's state to "not ready" (so that the agent does not get more calls) and launch a route request to find another agent. Any call data is preserved and popped onto the next agent's desktop. If no agent is available, the call can be sent back to the IP IVR for queuing treatment again. Again, all call data is preserved. The routing script for this RONA treatment should set the call priority to "high" so that the next available agent is selected for this caller. In the agent desk settings, you can set the RONA timer and optionally the DN used to specify a unique call type and routing script for RONA treatment.

In Order to configure RONA complete these steps:

1. In the ICM Script Editor, open the applicable script, and enable router requery on the Queue to Skill Group node.
2. Under the Agent Desk Settings configuration, set the **Ring No Answer Time** to the maximum time you want to allow the agent to answer the call. For example, set this to eight seconds to give the agent two rings before the call is rerouted through RONA. This timer must be shorter than the no answer time-out for router requery. See step 4.
3. Use the **DN Pattern Outbound Invite Timeout** option in the CVP Operations Console's SIP Service configuration tab in order to add the expiration timeout for a particular dialed number pattern.



4. Ensure that the **No Answer Ring Duration** on the DN in Cisco Unified Communications Manager is set to a value higher than the Cisco Unified Customer Voice Portal timeout timer. The default for this in Cisco Unified Communications Manager is 20 seconds.

The timer hierarchy for these three settings looks like this:

Agent Desktop < CVP Invite Timeout < Cisco Unified Communications Manager CFW Example: 10 seconds < 12 secs < 20 seconds CFW

### 7.3.4 Peripheral Gateway (PG) Installation

Each contact center device (ACD, PBX, or IVR/VRU) communicates with ICM software through a Peripheral Gateway (PG). The PG reads status information from the device and passes it back to the ICM software. The PG runs one or more Peripheral Interface Manager (PIM) processes, which are the software components that communicate with proprietary ACD and IVR/VRU systems.

Before you install a Peripheral Gateway (PG), the Windows operating system (for version specifics refer to the Cisco Intelligent Contact Management Software Release 9.0(1) Bill of Materials—including SNMP and (for Windows 2008 R2) WMI—must be installed on the computer, you must have setup the Windows Active Directory services for ICM software, and you must have setup at least one ICM instance.

Further, before you can complete the installation of a Peripheral Gateway, you must create configuration records in the ICM database. To create these configuration records you must have installed the Call Router, a Logger, and the Admin Workstation.

To configure a PG, you must know the visible network addresses for the Call Router machines. If the PG is duplexed, you must know the visible and private network addresses of its duplexed peer.

On the servers selected for the peripheral gateways start the ICMSetup.exe application. At least one ICM instance must be added before you can install any ICM components.

In the Cisco ICM Setup dialog box, in the ICM Instances section, click Add. The Add Instance dialog box opens.

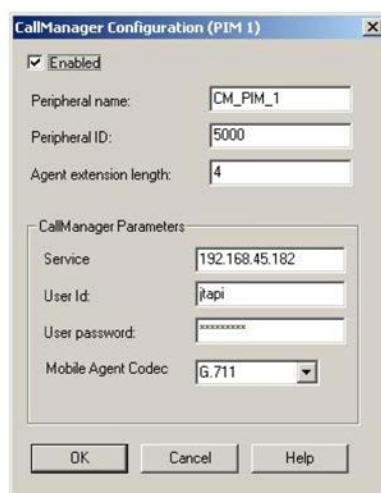
Complete the following steps:

1. Select the network Domain for the instance.
2. Select the Facility Organizational Unit for the instance.
3. Select the Instance Name for the instance.
4. Use the Instance Number generated by the ICM software. (For standard single-instance ICM configurations, the instance number is 0.)
5. Click OK.

#### PG Installation Steps

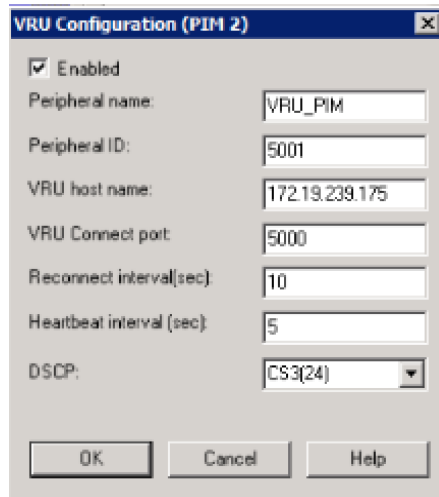
1. In the ICM Setup application, click the Add button on the right under Instance Components.

2. A new dialogue window will appear where you will be able to select the Peripheral Gateway component. In the Peripheral Gateway properties window configure the following:
  - a. Check the Production node.
  - b. Check the Auto start at system startup.
  - c. Check the duplexed Peripheral Gateway.
  - d. Set the PG Node Properties ID to PG 1 and select the appropriate side for duplexed installations.
  - e. Select the following client types and click the Add button:
    - Call Manager
    - VRU
  - f. Click Next.
3. For the Peripheral Gateway Component Properties click Add in the Peripheral Interface Managers section.
4. Set the Client type as Call Manager and select PIM 1 from the Available PIMS List. Click OK.
5. In the PIM Configuration dialogue, configure the PIM as follows:
  - a. Select Enable.
  - b. Enter an appropriate Peripheral name.
  - c. Enter the Peripheral ID that was assigned by the Configuration Manager on the Admin Workstation.
  - d. Specify the appropriate agent Extension length for DN's on the Cisco Unified Communication Manager (this is critical as additional digits are added for call handling to CVP and call handoff will fail when mismatched).
  - e. In the Call Manager Service Parameter enter the IP address of the call manager cluster publisher.
  - f. Enter the CCE username and password created in the Call Manager (i.e. jtapi user).
  - g. Click OK.



6. Back on the Peripheral Gateway Component Properties click Add in the Peripheral Interface Managers section again. Set the Client type as VRU and select PIM 2 from the Available PIMS List. Click OK.

7. In the PIM Configuration dialogue, configure the PIM as follows:
  - a. Select Enable.
  - b. Enter an appropriate Peripheral name.
  - c. Enter the Peripheral ID that was assigned by the Configuration Manager on the Admin Workstation.
  - d. In the VRU Hostname enter the IP address of the CVP Server.
  - e. Enter VRU connection port.
  - f. Click OK.



8. Back on the Peripheral Gateway Component Properties enter the Peripheral Gateway Logical controller ID that was generated by the Configuration Manager on the Admin Workstation and click Next.
  9. On the Device Management Protocol Properties set Side A preferred option and click Next
  10. Enter the name or IP addresses for the Visible and Private Interfaces of the PG and Router. Optionally, enable QoS for these interfaces as desired. Click Next.
  11. Review the PG setup information and click Next to complete installation of the first PG.
- Peripheral Gateways

### 7.3.5 JTAPI Client Installation

It is mandatory to install the JTAPI client on the CUCM PG (which is PG1 in this setup) machine, so that it can talk to the CUCM via JTAPI interface. Once this has been completed, there will be a new process called JTAPIGW, which should be active even if no agents or phones are created in the CUCM.

Associate all of the agent's phone devices with this user in CUCM as well. To install the jtapi client, download the client from the CUCM administration interface and install it on the PG1 machine.

Cisco Unified CM Administration For Cisco Unified Communications Solutions		
System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾		
Find and List Plugins		
Find plugin where (Name) [ ] and plugin type equals (Installation) [ ]		
	Plugin Name ^	Description
<a href="#">Download</a>	<a href="#">Cisco AXL Toolkit</a>	Cisco Administrative XML (AXL) Toolkit enables Developers to create applications that create, read, update and delete Publisher. The zip file contains Java-based libraries that use SOAP over HTTP/HTTPS to send and receive AXL request where AXL applications will be developed. SHA1(/usr/local/thirdparty/jakarta-tomcat/webapps/plugins/axltoolkit.zip)= a8:10:8c:43:1a:ec:d7:7c:10:19:11:f
<a href="#">Download</a>	<a href="#">Cisco CTL Client</a>	Install the Cisco Certificate Trust List (CTL) client to digitally sign certificates stored on the TFTP server. The client ret CTL file using a security token and then updates the file on the Cisco TFTP server. Install this plug-in on Windows 32-bit. SHA1(/usr/local/thirdparty/jakarta-tomcat/webapps/plugins/CiscoCTLClient.exe)= cd:9f:82:46:b9:f1:da:35:5d:58:4
<a href="#">Download</a>	<a href="#">Cisco IP Phone Address Book Synchronizer</a>	Cisco IP Phone Address Book Synchronizer enables users to synchronize their Microsoft Windows Address Book with t operating system computers for Users who desire to synchronize their Windows Address Book with their Cisco Unified SHA1(/usr/local/thirdparty/jakarta-tomcat/webapps/plugins/TabSyncInstall.exe)= 16:0e:b3:58:51:1d:36:f0:87:e3:c
<a href="#">Download</a>	<a href="#">Cisco JTAPI 32-bit Client for Linux</a>	JTAPI provides a standard programming interface for communication-enabled applications that interact with Cisco Unified Communication sample code are included. SHA1(/usr/local/thirdparty/jakarta-tomcat/webapps/plugins/CiscoJTAPIClient-linux.bin)= 9e:7e:d6:ac:2c:1e:ca:02:6
<a href="#">Download</a>	<a href="#">Cisco JTAPI 32-bit Client for Windows</a>	JTAPI provides a standard programming interface for communication-enabled applications written in the Java program system computers which host communication-enabled CTI applications that interact with Cisco Unified Communication sample code are included. SHA1(/usr/local/thirdparty/jakarta-tomcat/webapps/plugins/CiscoJTAPIClient.exe)= 2f:8b:2a:91:78:83:6b:f0:c4:68:
<a href="#">Download</a>	<a href="#">Cisco JTAPI 64-bit Client for Linux</a>	JTAPI provides a standard programming interface for communication-enabled applications written in the Java program system computers which host communication-enabled CTI applications that interact with Cisco Unified Communication sample code are included. SHA1(/usr/local/thirdparty/jakarta-tomcat/webapps/plugins/CiscoJTAPIx64-Linux.bin)= a8:e4:e7:3a:a8:f1:09:03:f9
<a href="#">Download</a>	<a href="#">Cisco JTAPI 64-bit Client for Windows</a>	JTAPI provides a standard programming interface for communication-enabled applications written in the Java program system computers which host communication-enabled CTI applications that interact with Cisco Unified Communication sample code are included. SHA1(/usr/local/thirdparty/jakarta-tomcat/webapps/plugins/CiscoJTAPIx64-Windows.exe)= 34:cb:ac:ee:29:52:93:3
<a href="#">Download</a>	<a href="#">Cisco TAPI 32-bit Client</a>	TAPI provides a standard programming interface for communication-enabled applications running on Microsoft Windows computers which host communication-enabled CTI applications that interact with Cisco Unified Communications Manager applications to play announcements and record call media. SHA1(/usr/local/thirdparty/jakarta-tomcat/webapps/plugins/CiscoTSP.exe)= e6:6c:30:b2:05:3b:aa:39:d6:be:8f:ae:
<a href="#">Download</a>	<a href="#">Cisco TAPI 64-bit Client</a>	TAPI provides a standard programming interface for communication-enabled applications running on Microsoft Windows 64-bit operating system computers which host communication-enabled CTI applications that interact with Cisco Unified enable TAPI-based applications to play announcements and record call media. SHA1(/usr/local/thirdparty/jakarta-tomcat/webapps/plugins/CiscoTSPx64.exe)= eb:a2:f5:51:48:18:db:16:92:a1:45
<a href="#">Download</a>	<a href="#">Cisco TAPS</a>	Cisco Tool for Auto-Registered Phone Support (TAPS) helps Users remotely download preconfigured phone settings to Administration, Unified CM Administration and Unified Contact Center Express (UCCX). Install this component on a UC Communications Manager release. SHA1(/usr/local/thirdparty/jakarta-tomcat/webapps/plugins/TAPS_AAR.aar)= 56:42:65:96:15:4a:0e:d9:a0:61:a4:7

Within the Cisco Unified CM Administration interface select Application and then Plugins. Click the Find button to list all available plug-ins. Download and install the Cisco JTAPI for Windows plug-in.

After completion of the JTAPI plug-in, install the CTI Server.

### 7.3.6 CTI Server Installation

Cisco supports installation of CTI Server on the same machine where the Peripheral Gateway software is installed. Installing CTI Server on a machine separate from the PG may cause network problems including, but not limited to, network disconnects, agents missing calls, and agents forced into **Not Ready**.

Before installing CTI Server, you must have installed/set up all the other components of ICM as described in the preceding sections.

CTI Server (*ctisvr*) is also called CG (short for CTI Gateway), which connects to the CTI OS Server using the *ctidriver* service running on the CTI OS Server machine.

In the ICM Setup application, click the Add button on the right under Instance Components.

A new dialogue window will appear where you will be able to select the CTI Server component.

In the CTI Server properties window configure the following:

1. Check the Production node.
2. Check the Auto start at system startup.
3. Check the duplexed Peripheral Gateway.
4. Set the CG Node Properties ID to CG 1 and select the appropriate side for duplexed installations.
5. Click Next.
6. CTI Server as a default connects to the CTIOS Server on port 42027, but can be configured to use a different port. Click Next.
7. Configure the PG and CG Public and Private interfaces. Click Next.
8. Review the CG setup information and click Next to complete installation of the CTI Gateway.

### 7.3.7 CTI OS Server Configuration

The Computer Telephony Integration Object Server (CTI OS) is Cisco's next generation customer contact integration platform. CTI OS combines a powerful, feature-rich server and an object-oriented software development toolkit to enable rapid development and deployment of complex CTI applications.

Refer to the [CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions](#) for a complete explanation of configuring peripherals and connection profiles in the CTI OS Server.

From the Server directory on the CD, run Setup.exe (or if already installed C:\icm\CTIOS\_bin\setup.exe). Click Yes on the Software License Agreement screen. The CTI OS Instances dialog appears.

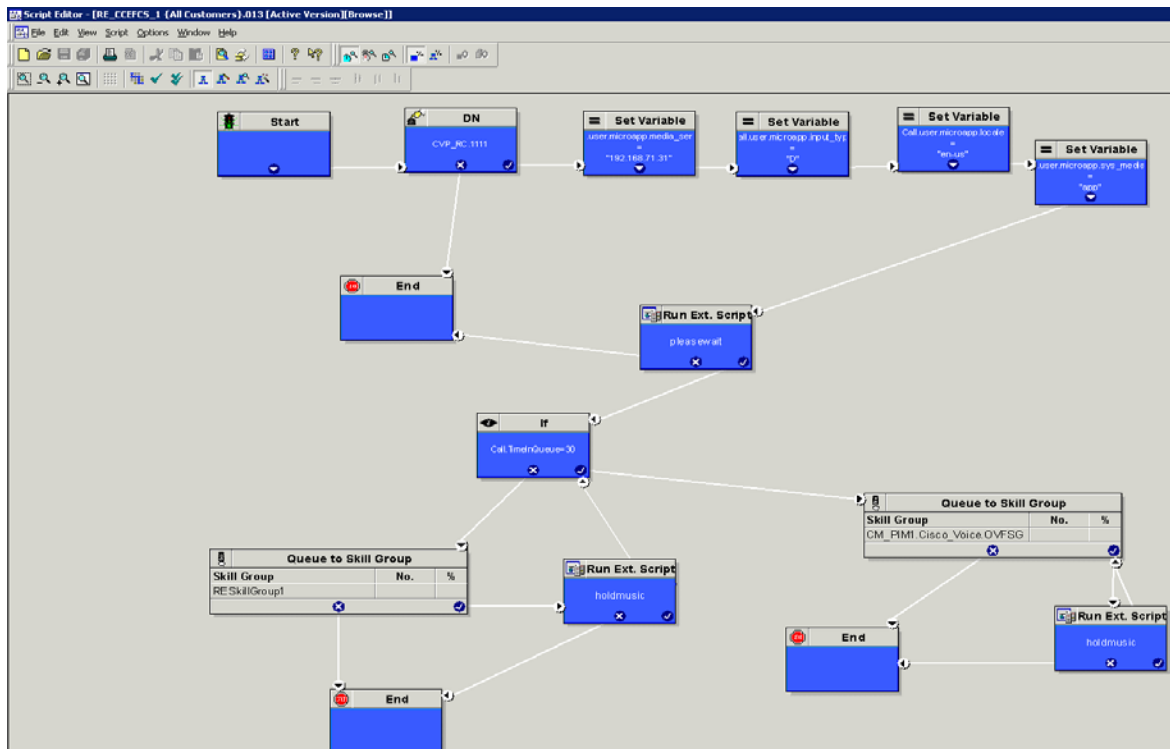
1. The CTIOS Instances dialog allows you to create CTI OS Instances and add CTI OS Servers to a configured instance of CTI OS. You will create only one CTI OS instance for each ICM instance.
2. Under the CTI OS Instance List, click Add.
3. Enter an instance name (e.g., "ctios").
4. Now click on Add inside the CTI OS Server List. The Add CTIOS Server dialog appears.
5. The CTIOS Server Name is filled in with the string "CTIOS" followed by the next available index for a CTI OS Server. If a CTI OS Server has been deleted, the CTIOS Server Name string is filled in with the index that was deleted.
6. If you are installing CTI OS Server for the first time, an Enter Desktop Drive screen appears. Accept the default installation drive or select another drive from the pull down list.
7. The Peripheral ID here is the same ID that was assigned during the CUCM PG configuration in the Configuration Manager on AW. The agent desktop communicates with the CUCM IP Phone.
8. The listen port is where CTI Desktop Agent will connect. This port will also be used if a secondary CTIOS Server wants to talk to this one in an high availability environment or setting.
9. Enter the default-polling interval for Skill group statistics (in seconds). Click Next.
10. The Peer CTIOS Server dialog is used to configure a CTI OS Peer Server. It is also used for Chat and CTI OS Silent Monitoring. Enter the appropriate information. After you click Finish, and the files are laid down, the service is registered, and Registry entries are made.
11. The Security installation is launched.
12. If you wish to disable Security, just click OK; otherwise, check the checkbox and enter the appropriate information, and click OK.

Upon the completion of the CTI OS Server the next step is to create device targets in Configuration Manager. Device targets are the extensions used by the formal Contact Center agents when the login into the Agent Desktop application. These next configuration steps are for formal contact center agents that would be used in addition to the Expert advisor agents. It is recommended to install a few formal agents for testing prior to the completed Expert Advisor implementation.

### 7.3.8 ICM Script

Create and schedule a routing script on AW by using the Script Editor software. The logic that is followed for creating this script is as follows:

1. Start the script with the start node.
2. Set the value of DN node to the suitable VRU\_RC (the pilot point DN), which would match the dialed number, sent to ICM by CVP.
3. Set the value of media server HTTP URL in Call.user.microapp.media\_server variable. This is the web server URL from where .wav files will be played (e.g., <http://media.cisco-irn.com>).
4. Set the value of language in Call.user.microapp.locale as en-us.
5. Set the value of input type (which is digits in this sample script) in Call.user.microapp.input\_type variable to D.
6. Set the value of the Call.user.microapp.app\_media\_lib to app.
7. After setting the variables send the call to IVR using "Run External Script" node.
8. Run external script called "silence" that will play the silence tone to the customer when the customer is put in queue. This is done because, in Remote Expert, there is a Video In Queue (ViQ) being configured which plays video and audio to the Customer while in queue and setting any other media file here would conflict with the desired ViQ being played back to the customer.
9. Use an "If" node to determine if the call stays in the queue for longer than x seconds and send the call to a different skill group if the condition is met. Send false condition to skill group with experts configured with video capabilities and True condition to skill group with audio only experts for example.
10. In either case, send the call to "Queue to skill group" node and select the desired skill group.
11. Add "Run external script" and "Release Call" nodes from the Queue to skill group node for both success and failure conditions respectively. If the call is queued and no agent is in "Ready" state the call will be queued and the media file configured in "Run external script" node will be played to the customer.



Once the script has been complete, it needs to be activated. Follow the steps below to activate the script:

1. Pull Down 'Script' menu and select 'Call Type Manager'.
2. Select 'Dialed Number'. Add or Modify.
3. Select 'Call Type'
4. Select 'Schedule' and select schedule and script. Add/Modify to select script / period.

## 7.4 Component Checkpoint: Verify UCCE component integration

- Verify UCCE Node -> Diagnostic framework shows all processes with healthy status.
- Verify SQL installation went through successfully on Logger and AWHDS
- Verify that you are able to login to the database on Logger and AWHDS
- Verify that AWHDS is able to open configuration manager.
- Verify that when you open the script manager you do not get an error – this confirms that the AW distributor is alive and talking clean with the UCCE Logger.
- Verify integration of UCCE components

## 7.5 Troubleshooting

### 7.5.1 Service Temporary Unavailable message displayed instead of the Login page

Problem Summary	Service Temporary Unavailable message is displayed in the web browser; the Login page is not displayed.
-----------------	---

Error Message	Service Temporary Unavailable! The server is temporarily unable to service your request due to maintenance downtime or capacity problems. Please try again later.
Possible Cause	Tomcat goes down while the browser is open to the Login page.
Recommended Action	Refresh your browser. If still unsuccessful, ensure that the Apache Tomcat 7 service is running.
Release	9.0(1)
Associated CDETS #	None.

### 7.5.2 Unified CCE Admin does not Display Properly in IE9

Problem Summary	Unified CCE Administration does not display properly/has graphical glitches when viewed in the Internet Explorer 9 (IE9) web browser, but works fine in Mozilla Firefox.
Error Message	N/A
Possible Cause	IE9 Compatibility View settings are not configured correctly.
Recommended Action	1) Using the IE9 web browser, select the <b>Alt</b> key to show the Tools menu. 2) Select <b>Compatibility View Settings</b> from the Tools menu and make sure that the <b>Display Intranet Sites in Compatibility View</b> check box is unchecked.
Release	9.0(1)
Associated CDETS #	None.

### 7.5.3 Logger processes crashes after upgrade to SQL Server 2008 R2

Problem Summary	After you upgrade from SQL Server 2005 to SQL Server 2008 R2, the logger processes crashes.
Error Message	from the clgr log:  SQL Server User Error: 229, State 5, Severity: 14, Message: The



	SELECT permission was denied ... dbselexec failed.
Possible Cause	Missing BUILTIN\Administrators users or missing server role "sysadmin" for BUILTIN\Administrators
Recommended Action	Manually add BUILTIN\Administrators: <ol style="list-style-type: none"> <li>1. Open SQL Server Management Studio.</li> <li>2. Go to Security &gt; Logins.</li> <li>3. Add New Login for BUILTIN\Administrators.</li> <li>4. Select "sysadmin" for Server Roles for BUILTIN\Administrators.</li> </ol>
Release	9.0(1)
Associated CDETS #	

#### 7.5.4 SQL Server 2008 R2 fails registry key validation

Problem Summary	Consistency validation for SQL Server 2008 registry key fails
Error Message	The SQL Server 2008 R2 installation log includes the following error:  Could not fix registry key HKEY_LOCAL_MACHINE\Software\Microsoft\MSSQLServer\Client\DB-Lib
Possible Cause	Registry hive permission
Recommended Action	Before you install SQL Server 2008 R2, you must grant access permission to the <b>BUILTIN\administrators</b> group for the following registry key under <b>Wow6432Node</b> : HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\MSSQLServer\Client\DB-Lib
Release	9.0(1)
Associated CDETS #	None

#### 7.5.5 Un-Installing SQL Server 2005 32 bit and Installing SQL Server 2008 64 bit

Upgrading a SQL 2005 32 bit to SQL 2008 64 bit is not supported. The following procedure details how to migrate from SQL 2005 to SQL 2008.

- Take a backup of all ICM databases (SideA/sideb, AW, HDS, baA) using CGUpgradeBackup.exe.
  - Go to command prompt and execute the below command :
  - CGUpgradeBackup -backup -sh <your backup folder name>
- Un-install 32 bit SQL Server 2005 completely from the system.
- Install SQL Server 2008 64 bit followed by Service Pack 1. Refer to [How to install SQL Server 2008 64 bit for installation steps.](#)
- Open SQL Server 2008 Management studio, select No for Import customized user setting from SQL 2005 and SQL 2005 management studio registered servers dialog.
  - (These dialog windows appear for the first time when SQL Server 2008 Management Studio is opened.)
- Restore the SQL db of all the db's (SideA/sideb, Aw, HDS, baA) into SQL Server 2008 Management Studio by using CGUpgradeBackup.exe.

Go to command prompt and execute the below command:

CGUpgradeBackup -restore -sh <your backup folder name>

## 8 Cisco Agent Desktop Services

---

In this section, we assume that CAD Desktop services 9.0 platform is already installed. If not, please refer to the [CAD 9.0 installation guide](#) available on Cisco.com.

Some pre-requisites are listed below:

1. For CAD 9.0 applications to work properly your agents must be organized into teams and some must be designated as supervisors. This is accomplished in Unified ICM. See your Unified ICM documentation for information on how to do this.
2. In order to correctly display enterprise data and call history in CAD, you must enable the “Permit application routing” option. This option is located on the List Tools > Dialed Number/Script Selector List node in ICM Configuration Manager.
3. When creating skill groups, the Skill Group ID must not be 0 (zero) in order for statistics to populate properly in Supervisor Configuring Unified ICM Desktop. In Unified ICM Configuration Manager this ID is known as the Skill Group Peripheral ID.
4. Make the server (both servers in an HA environment) on which you are going to install the CAD base services a member of a domain. The server on which you install the CAD base services must be a member of a domain, not of a workgroup. If you change the domain after the services are installed, or switch from workgroup to domain, you must reinstall the CAD base services in order to avoid problems with partial or no service when running the CAD desktop applications.
5. Create a user account (on both servers) in Windows Computer Management with the following requirements:
  - The user must have local administrator privileges.
  - The user account must have a password. If either of the servers does not have a password, replication setup will fail because the subscriber cannot connect to the publisher to configure the replication.
  - The same user account must exist on the ICM Admin Workstation computer.
  - The user must have read privileges for the ICM Admin Workstation database.
  - This user account must be used to install SQL Server 2008 R2 and also to install the CAD base services on both Side A and Side B.
6. You must configure the Sync service to connect to the Admin Workstation SQL database via a TCP/IP connection. Run the SQL Server Network Utility on the Admin Workstation machine. On the General tab, ensure that TCP/IP is enabled.

### 8.1 Configuration

The basic configuration for the CAD Desktop services is explained under the [CAD Configuration setup utility in the CAD 9.0 installation guide](#). However we will browse through some quick steps and screenshots in this space below. Complete the following procedure if you are running the CAD Configuration Setup utility for the first time on a single server system or on the primary server (Side A) in a replicated system.

## Steps

The Cisco Agent Desktop Configuration Setup utility starts automatically and displays the Location of CAD Base services dialog. Enter the IP address of the primary CAD base services and then click OK. The CAD Configuration Setup utility appears. Complete the fields for each node, using the right arrow on the toolbar or Ctrl+N to move forward to the next node.

You cannot move forward until all required information is entered. You cannot skip a node. You can go backwards using the left arrow or Ctrl+B at any time to revisit a previous node. The Save button is only enabled when all nodes are completed. When you have completed all nodes, click Save on the toolbar or choose File > Save.

When the data is successfully saved, the utility ends automatically. The save process can take several minutes. Once your configuration settings have been saved, Unified CCE License Administration will launch automatically. Refer to "Licensing CAD 9.0" for more information. You only have to complete this step on Side A.

### 8.1.1 Unified CM SOAP AXL Access

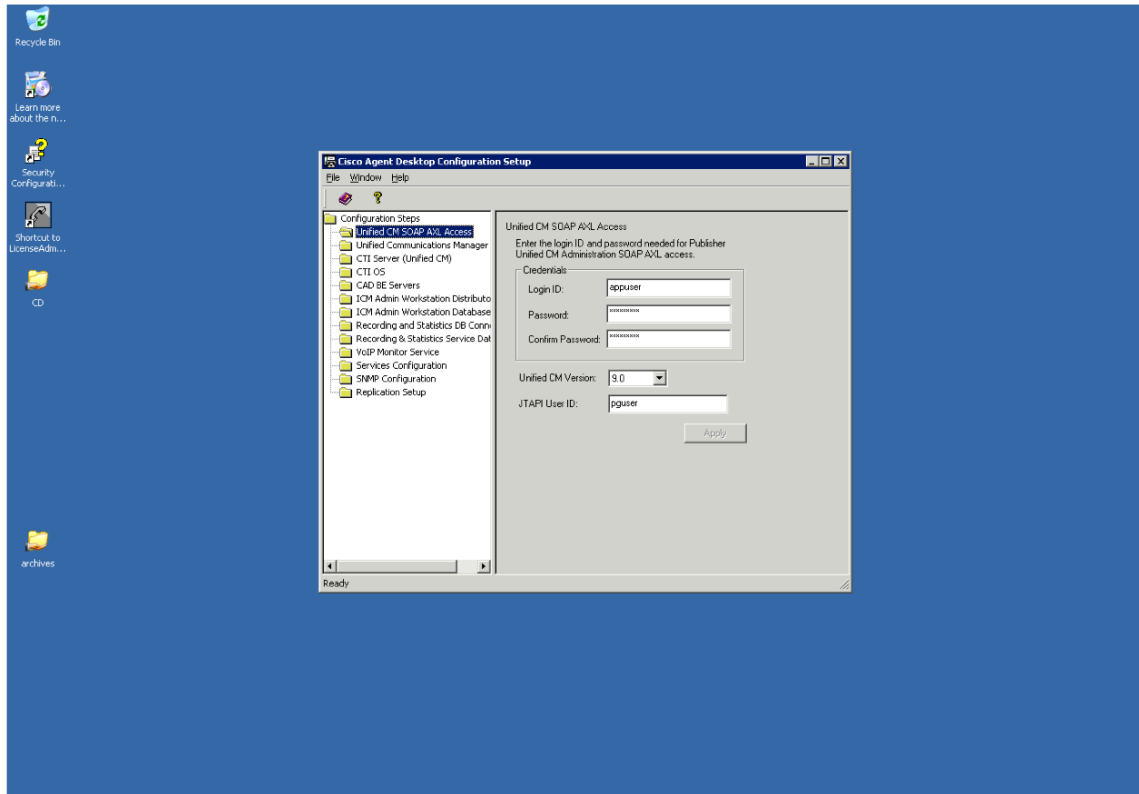
Enter the login ID and password required for the publisher Unified CM Administration to access Unified CM SOAP AXL (Simple Object Access Protocol Administrative XML Layer). The login ID and password are the same used to access the publisher Unified CM.

Enter the required JTAPI User ID, which is case sensitive. For more information about users in Unified CM, refer to the "Roles" section of the Cisco Unified Communications Manager System Guide.

For more information on the JTAPI user for Unified CM, refer to the "Configure users for phones, Unified CM PG, and Unified IP IVR" section of the Installation and Configuration Guide Cisco Unified Contact Center Enterprise. These documents are available on the Cisco website ([www.cisco.com](http://www.cisco.com)).

**NOTE:** The Unified CM Version drop-down list does not appear the first time you run the CAD Configuration Setup utility. It appears when you run the CAD Configuration Setup utility again to change your settings.

If you change these settings after initial setup, you must restart the Sync service and the VoIP Monitor service to ensure that the change is registered with them properly.



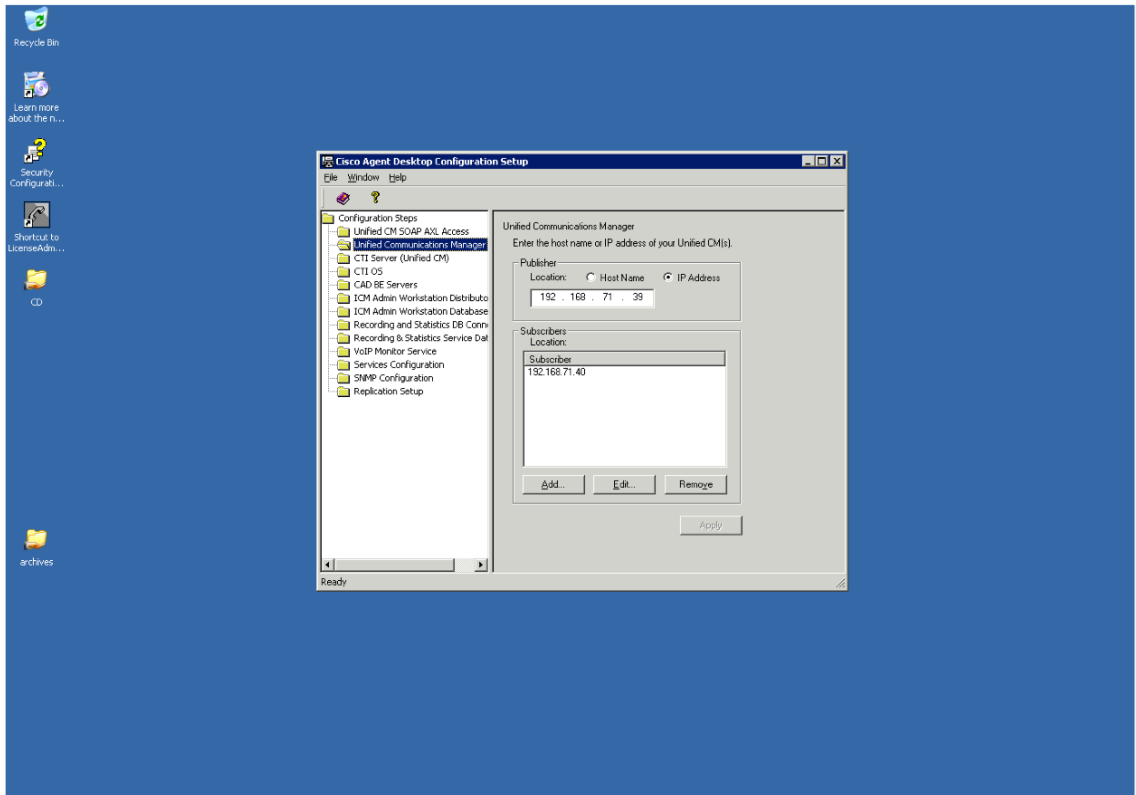
### 8.1.2 Unified Communications Manager

If you have only one Unified CM server, complete the Publisher section by selecting Hostname or IP Address. Then enter the location of the publisher Unified CM server.

Leave the Subscriber section blank. If you have a Unified CM cluster, complete the Publisher section and add the locations of all of the subscriber Unified CM servers in the Subscribers section. To add a subscriber location, click Add. The Add/Edit Host dialog box appears. Enter the location of the subscriber Unified CM server in one of the following ways, and then click Apply.

- Select Hostname, and then type the hostname of the subscriber Unified CM server.
- Select Hostname, and then choose the hostname of the subscriber Unified CM server from the drop-down list.
- Select IP Address, and then type the IP address of the subscriber Unified CM server.

**NOTE:** If you change these settings after initial setup, you must restart the Sync service and the VoIP Monitor service to ensure that any changes are registered with them properly.

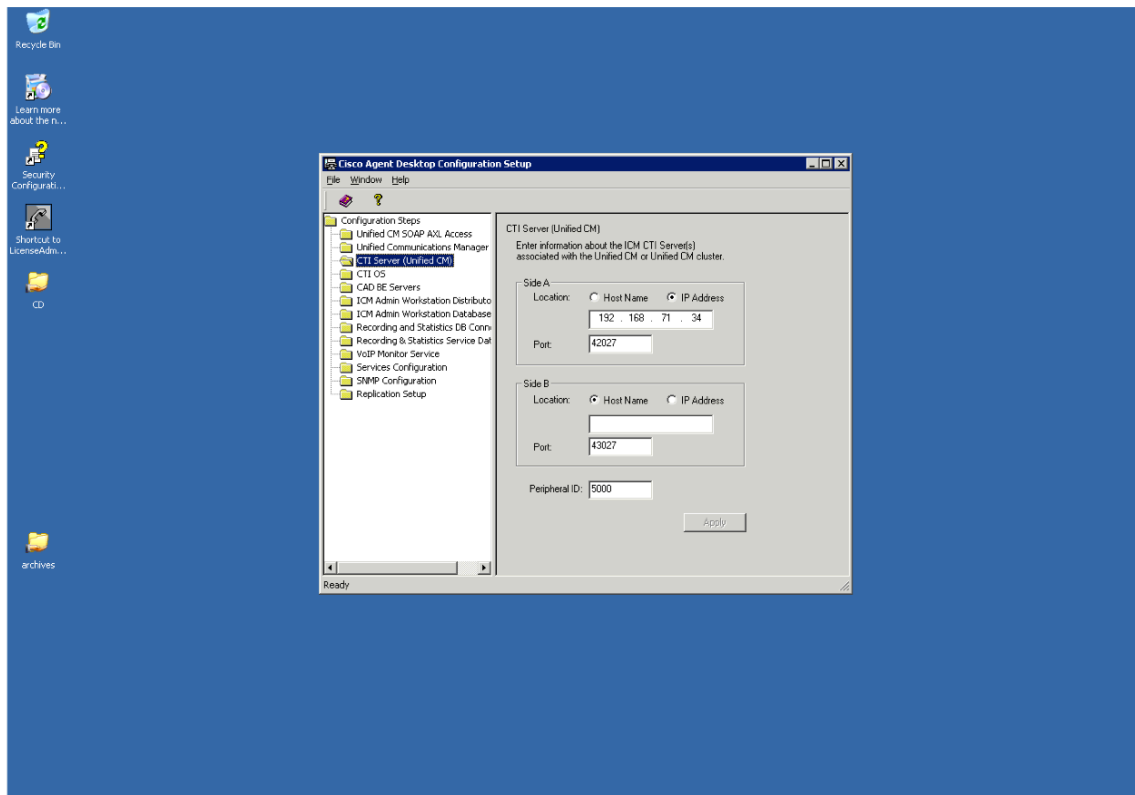


### 8.1.3 CTI Server (Unified CM)

Enter the hostname or IP address, port number, and peripheral ID of the Unified ICM CTI Server associated with the Unified CM or Unified CM cluster.

- If the CTI Server is entered with a hostname in Unified ICM, enter a hostname. If it is entered as an IP address, enter an IP address. Mixing hostname and IP address between Unified ICM and the CAD Configuration Setup utility can result in failing to display enterprise data in desktop applications.
- If you have only one Unified ICM CTI server, enter the information in the Side A section.
- If you are also using a redundant Unified ICM CTI server in a replicated environment, enter the location of the redundant Unified ICM CTI server in the Side B section.
- Enter the correct peripheral ID for your system. The default value is 5000. The peripheral ID is used by services to filter information such as agents and skills. You can find the peripheral ID for your system by using PG Explorer in the Unified ICM Configuration Manager.

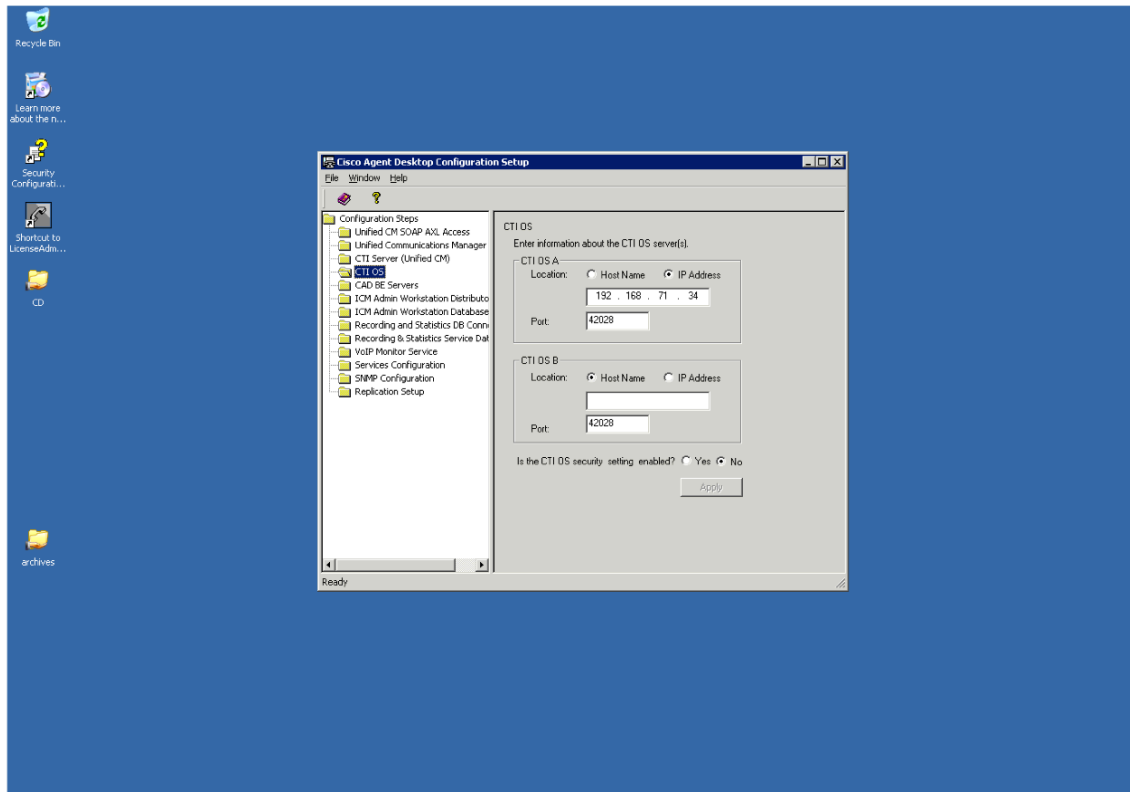
**NOTE:** If you change the peripheral ID, you must restart the Sync service, the Enterprise service, and the BIPPA service to ensure that the change is registered with them properly.



### 8.1.4 CTI OS

Enter the hostname or IP address and port number of the CTI OS (Computer Telephony Integration Object Server).

- If you have only one CTI OS, enter the information in the CTI OS A section.
- If you are also using a redundant CTI OS in a replicated environment, enter the location of the redundant CTI OS in the CTI OS B section.
- If you are running the CAD Configuration Setup utility for a second time to modify your settings, the following question appears:
- “Is the CTI OS Security Setting Enabled?”
- Select Yes or No. If you choose Yes, ensure that CTI OS security is enabled on the CTI OS server.



### 8.1.5 ICM Admin Workstation Distributor

Type the hostname or IP address of the ICM Admin Workstation (AW) Distributor.

- If you have only one ICM AW Distributor, complete the Primary section only.
- If you are using a secondary ICM AW Distributor, enter its location in the Secondary section.

#### Additional Considerations when Modifying Configuration Settings

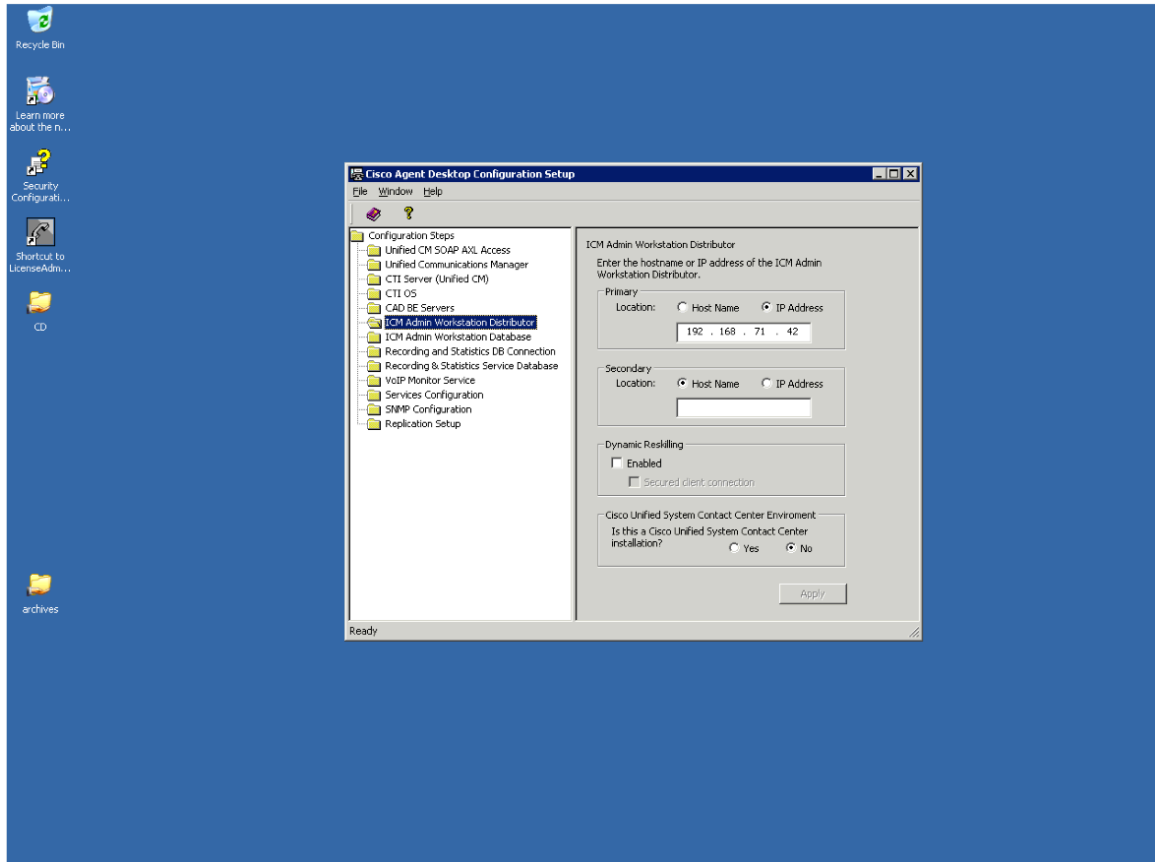
If you change either location after initial setup, you must restart each Recording and Statistics service and the Sync service to ensure that the change is registered with them properly.

The Dynamic Reskilling and Cisco Unified System Contact Center Environment sections appear only if you are running the CAD Configuration Setup utility a second time to change your configuration settings.

In the Dynamic Reskilling section, select the Enabled check box to enable supervisors to dynamically re-skill agents on their teams using the Unified Contact Center Enterprise Web Administration Agent Re-skilling tool. This tool is a web-based application. If it is located on a secured server and requires a secure socket URL (https), select the Secured client connection check box. If you leave this box unchecked, the URL will use the http prefix.

In the Cisco Unified System Contact Center Environment section, select Yes or No, to indicate whether or not your configuration is running in a Unified System Contact Center environment.



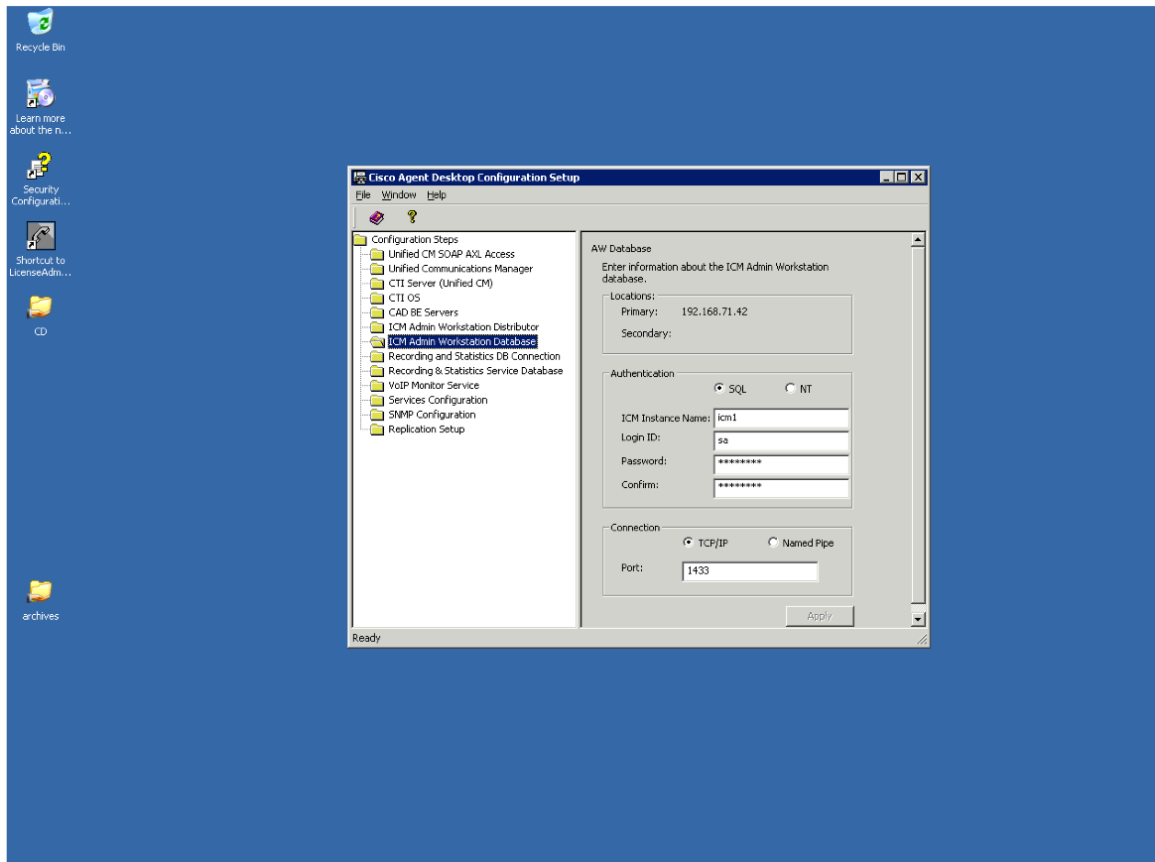


### 8.1.6 ICM Admin Workstation Database

The ICM Admin Workstation database locations are auto filled based on what you entered in the ICM Admin Workstation Distributor node.

Select NT authentication, and then enter the instance name and a user login ID/password. These fields are case sensitive.

**NOTE:** It is strongly recommended that you select NT authentication. SQL authentication appears for troubleshooting purposes only. This is the user account you created during your pre-installation preparation. The user must have read privileges for the ICM Admin Workstation database.



### 8.1.7 Admin Workstation computer

Select the connection type, TCP/IP or Named Pipes.

- If TCP/IP (recommended), enter the port number used to connect to the database.
- If Named Pipes, enter the share path in the format \\<path> in the Port field.

#### Additional Considerations for Modifying Configuration Settings

If you are using NT Authentication and change the ICM Login ID or Password on one side, the change will replicate to the other side. However, you must also run the CAD

Configuration Setup utility on the other side and click Apply to save this setting to ensure that the Windows Services user is updated properly also.

If you change the connection type settings after initial configuration, you must restart each Recording and Statistics service and the Sync service to ensure that the change is registered with them properly.

### 8.1.8 Recording and Statistics Database Configuration

Prior implementations of CAD 8.0, 8.5, and 9.0 supported the use of flat files or Microsoft SQL Server as the data store. As a matter of policy, effective immediately with release 9.0(3), all customers with new

deployments of any version of Cisco Agent Desktop must use SQL Server as the data store, and not flat files. The rationale behind this policy is that deployments with a fully replicated SQL Server database experience a more complete feature set and better performance and stability.

Customers who are upgrading to CAD 9.0(3) from a previous version of CAD that was run on Windows Server 2003 (CAD 7.5, 7.6, 8.0, 8.5(1), and 8.5(2a)) must migrate to SQL Server 2008 R2 as the data store.

Customers who used flat files with CAD 8.5(4) and CAD 9.0(1a) running on Windows Server 2008 R2 can continue to use flat files when upgrading to CAD 9.0(3), but are also encouraged to migrate to SQL Server 2008 R2. CAD documentation outlines the caveats associated with the use of flat files, including loss of functionality during fail over situations that might be caused by several reasons, network issues being the most common. Cisco Support and TAC reserves the right to request a migration to SQL Server 2008 R2 as a resolution plan.

If you are installing CAD 9.0(3) as a new deployment or if you are upgrading to CAD 9.0(3) from a version of CAD prior to 9.0, you must install CAD 9.0(1a) first and then install 9.0(3).

Unless the deployment meets one of the exceptions above, select Use SQL Server database.

#### Flat Files

Flat files are selected by default and the rest of the window is disabled. Continue to the next node.

#### SQL Server

Select Use SQL Server database, and enter the hostnames of the servers that host the primary and secondary Recording & Statistics service.

**NOTE:** Use the Host Name fields to connect to the database. The IP Address fields should not contain any data and are provided for troubleshooting purposes only.

You must have SQL Server 2008 R2 (64-bit) installed and configured on both servers. Select NT authentication, then complete the following fields:

It is strongly recommended that you select NT authentication. SQL authentication appears for troubleshooting purposes only.

- Instance Name: Enter the CAD SQL instance name.
- Database Directory: Verify the directory path to the CAD SQL instance database.

All SQL instances are installed to a default location. CAD assumes the SQL instance it is using is installed to this default location.

However, if you specified a name other than CADSQL for the SQL instance that CAD uses, the CAD SQL instance might be installed to a different location, which you must specify here.

If you enter a database directory that is not the default you must change it on both servers. It will not populate automatically to the other server.

Login ID/Password: Enter the login ID and password for the CAD SQL instance database. The user must have read privileges for the database.

The user must also have an account on the ICM Admin Workstation computer.

**NOTE:** If you selected NT Authentication for the ICM Admin Workstation database on the ICM Admin Workstation Database node, and select NT Authentication for the Recording and Statistics database here, then the username and password entered on the ICM Admin Workstation Database node is automatically brought forward and is read-only on this node.

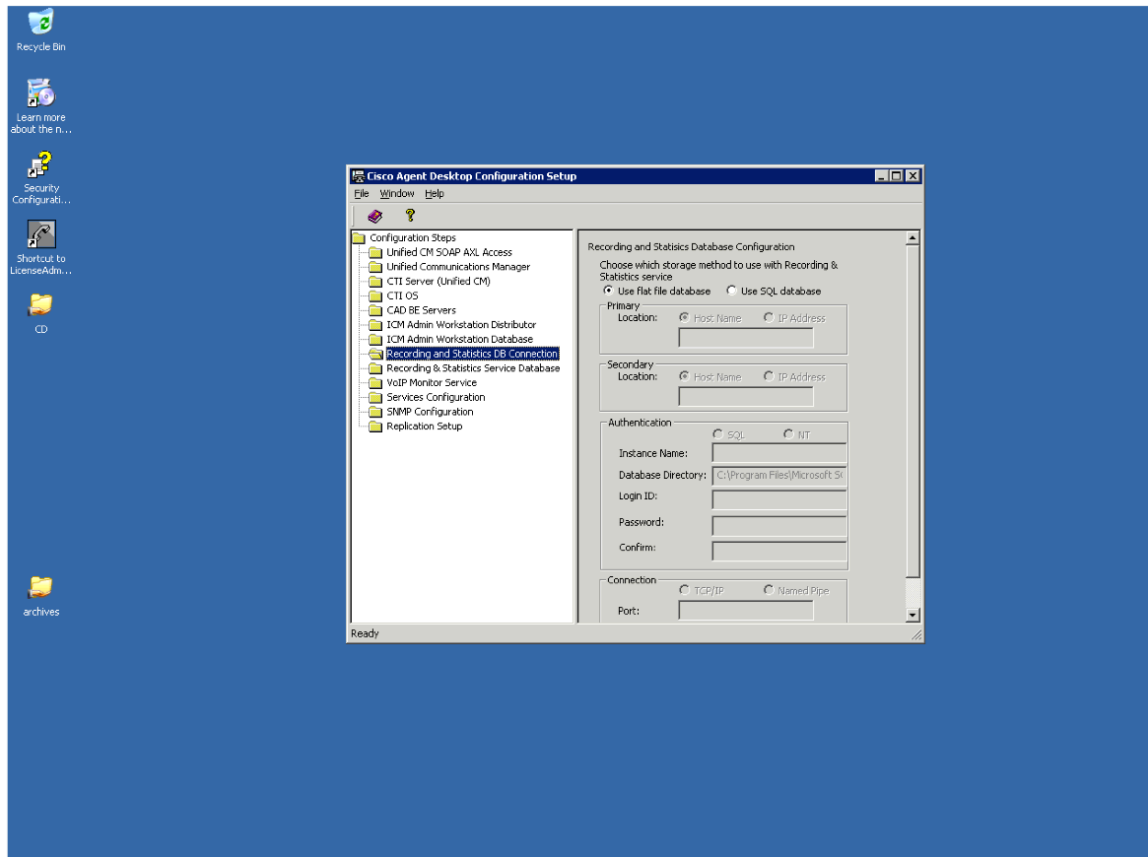
If the Login ID here is different than the ID used while installing SQL Server you must re-provision this new user as a sysadmin according to the instructions from the following article:

<http://msdn.microsoft.com/en-us/library/bb326612%28v=sql.105%29.aspx>

**NOTE:** If you change the Login ID/Password on one side, the change will replicate to the other side. However, you must also run the CAD Configuration Setup utility on the other side and click Apply to save this setting to ensure that the Windows Services user is updated properly also.

Select the connection type, TCP/IP (recommended) or Named Pipes. If you select TCP/IP, enter the port number used to connect to the database.

**IMPORTANT:** If you change any of the settings on this node after initial configuration, you must restart each Recording and Statistics service and the Sync service to ensure that the changes are registered with them properly.



### 8.1.9 Recording and Statistics Service Database

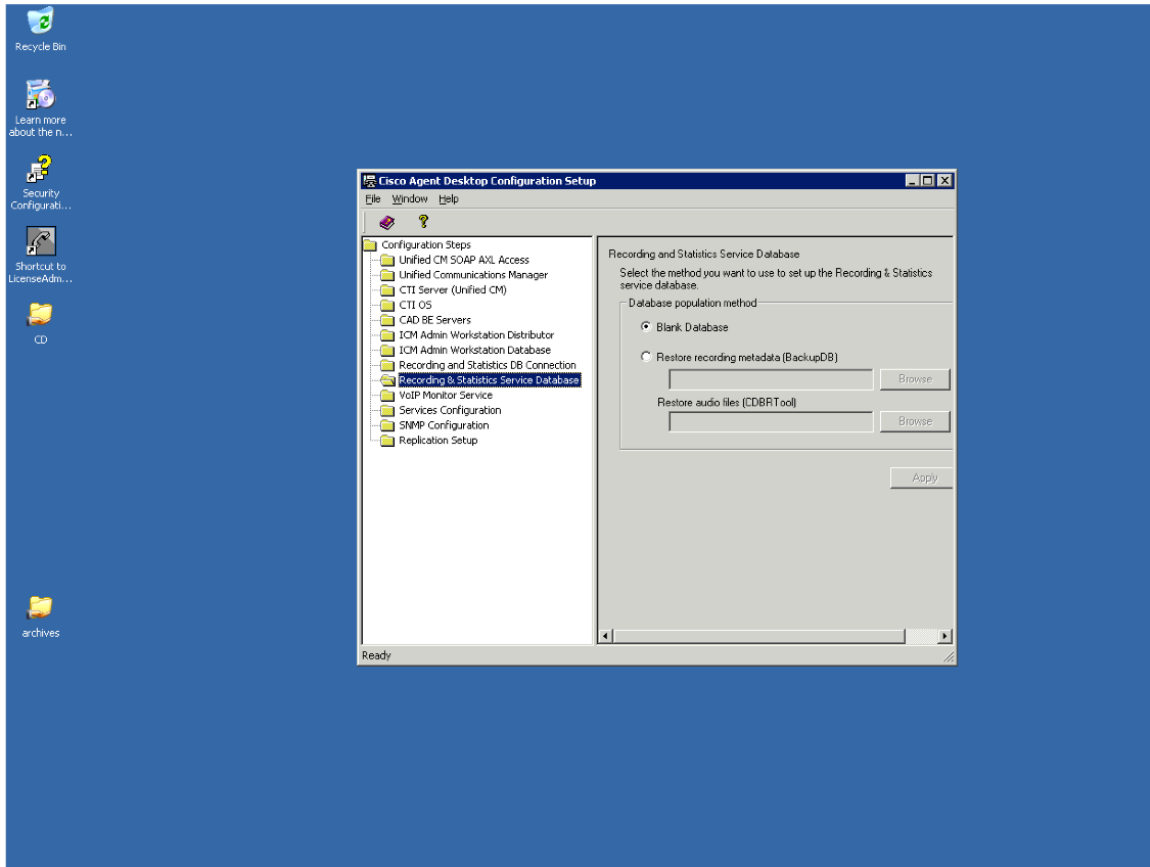
This step does not appear when running the CAD Configuration Setup utility on the secondary server in a replicated system, because the information was already entered on the primary system.

If you change these settings after initial setup, you must restart each Recording and Statistics service to ensure that the change is registered with them properly.

Select a method to set up the Recording and Statistics service database.

- Select Blank Database (default) if installing one service or a primary service in a replicated environment. This option creates the database schema.
- Select “restore from” if you are restoring a previously backed-up database. If you are running CAD in a replicated environment, a message appears, reminding you to shut down replication before restoring data. After dismissing the dialog box, click Browse to navigate to the backup database created with the BackupDB and CDBRTTool utilities. When you go to the next step, a message appears, reminding you to re-establish replication after the restore.

**NOTE:** You can restore recording metadata without restoring audio files, but you cannot restore audio files without recording metadata.



### 8.1.10 Restore Backup Data

This node appears only when the CAD Configuration Setup utility is run for the first time.

If you are upgrading and want to restore data that was saved from a previous version of CAD, select Yes. A dialog box appears reminding you to shut down replication before you start restoring backup data.

**NOTE:** If you do not shut down replication before restoring your data, your database will become corrupted. Click OK and then enter the path to the backup folder in the Backup Folder Location field. When you move to the next step or click Apply, a dialog box appears reminding you to re-establish replication after you exit the CAD Configuration Setup utility.

### 8.1.11 CAD-BE Servers

The CAD-BE Servers node only appears in when you run the CAD Configuration Setup utility again to change your settings.

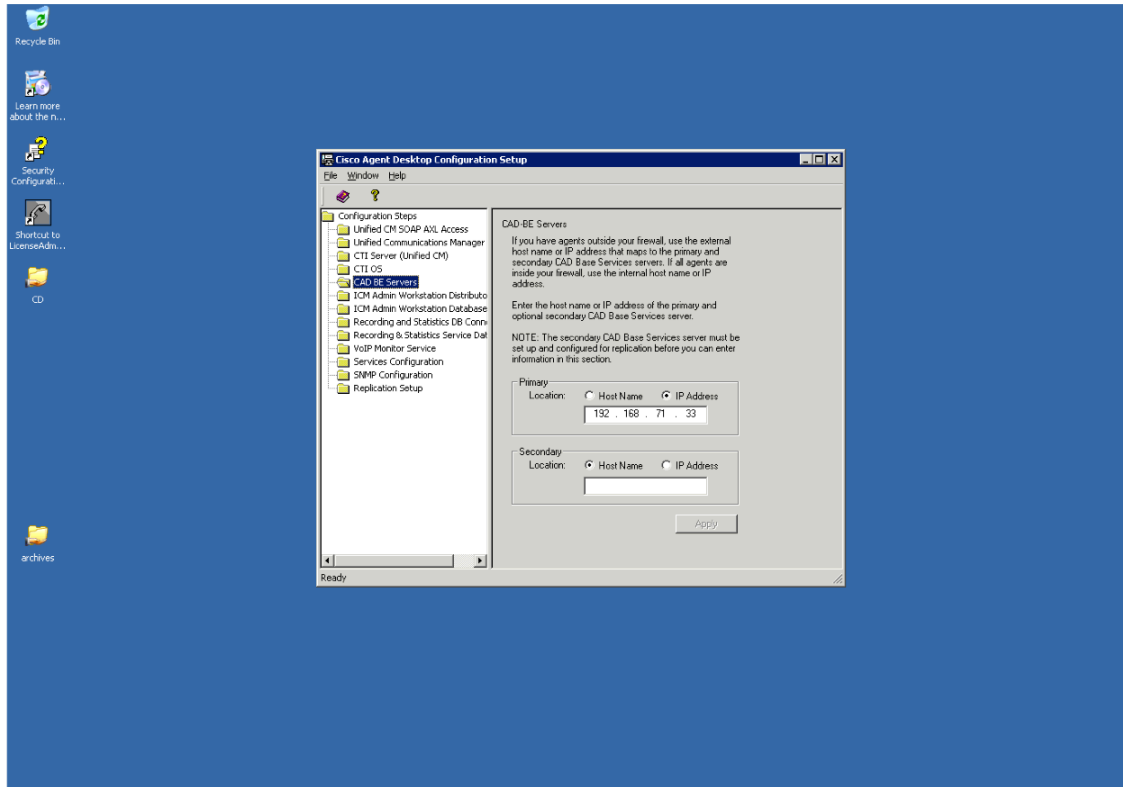
In the Primary Location field, type the hostname or IP address of the CAD base services server. Tomcat, which is required to run CAD-BE, is installed on this server.

If some of your agents are outside your firewall, use the external hostname/IP address that maps to the servers. If all of your agents are inside your firewall, use the internal hostname/IP address.

If your configuration includes a second server hosting the CAD base services, and you have configured replication between the two servers, enter the location of the second server in the Secondary Location field.

**NOTE:** If you are changing configuration settings and established replication in the first run of the CAD Configuration Setup utility, the Secondary Location field is filled automatically.

The Secondary Location is not enabled until you configure the second CAD base services server and establishes replication.



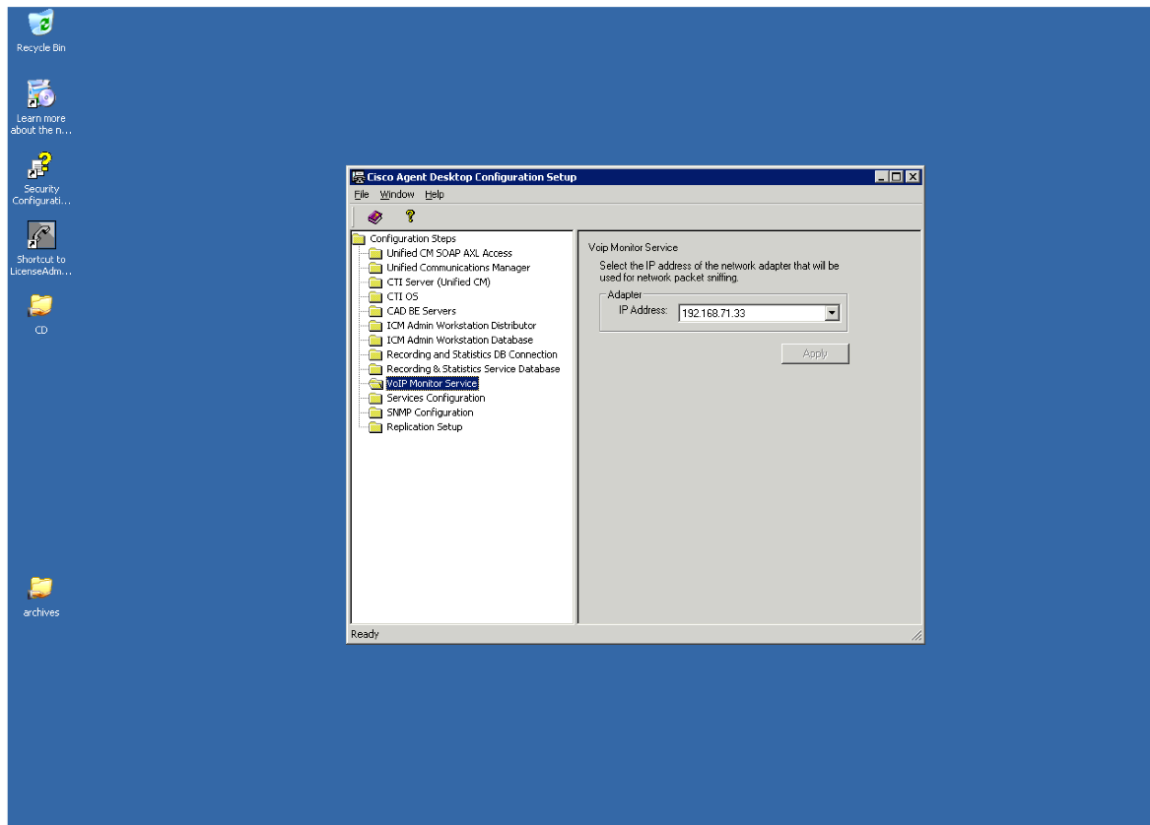
### 8.1.12 VoIP Monitor Service

The VoIP Monitor service node only appears when you run the CAD Configuration Setup utility again to change configuration settings.

Select the IP address of the network adaptor to which voice packets are sent to be sniffed by the VoIP Monitor service (if this is a server box) or the desktop monitor (if this is a client desktop).

- On a VoIP Monitor service server, it is the IP address of the NIC that is connected to the port configured for SPAN.
- On a client desktop computer, it is the IP address of the NIC on which the computer is daisy-chained to the phone.

**NOTE:** If you change these settings after initial setup, you must restart the VoIP Monitor service or the client application (depending on where you run the CAD Configuration Setup utility) to ensure that the change is registered with them properly.



### 8.1.13 Services Configuration

The Services Configuration node only appears when you run the CAD Configuration Setup utility again to change configuration settings.

If the computer has more than one IP address, select the IP address of the NIC used to connect to the LAN—it must be accessible by the client desktops.

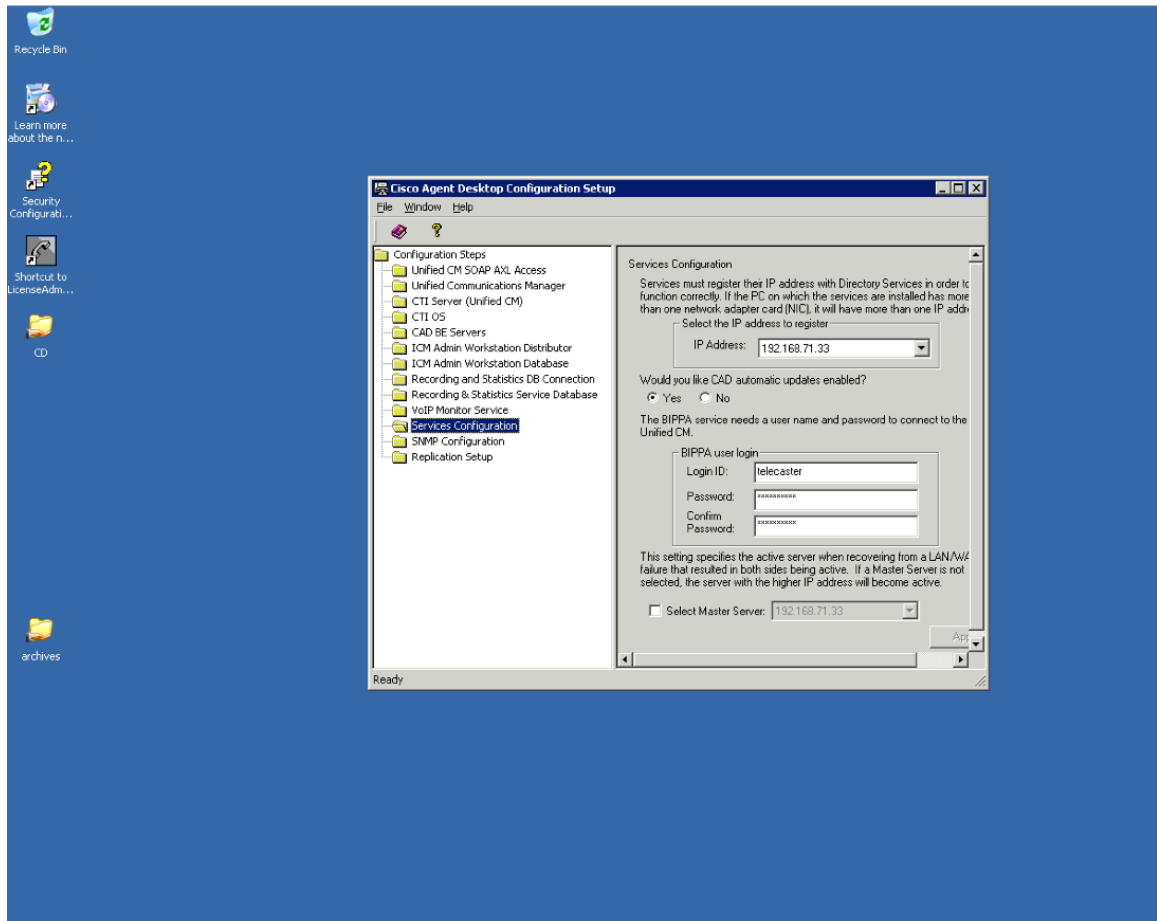
To enable CAD automated updates, select Yes. Automated updates cause Agent Desktop, Supervisor Desktop, and Desktop Work Flow Administrator to look for newer versions every time they start. If one is found, the update process is run automatically.

**NOTE:** To connect to Unified CM, the BIPPA service must have identical user IDs and passwords configured in this step and in Unified CM. You can complete the fields in this step before configuring the user in Unified CM.

- If you change any of these settings, you must restart all CAD services to ensure that the change is registered with them properly.
- If your system is High Availability over WAN/LAN, and you want to designate a master server, select the Select Master Server check box and then choose the appropriate IP address from the drop-down list.



- If the WAN link goes down, both servers think that the other server is down and try to take over as master server. When the link is restored, this setting dictates which server is the master and which server is on standby.



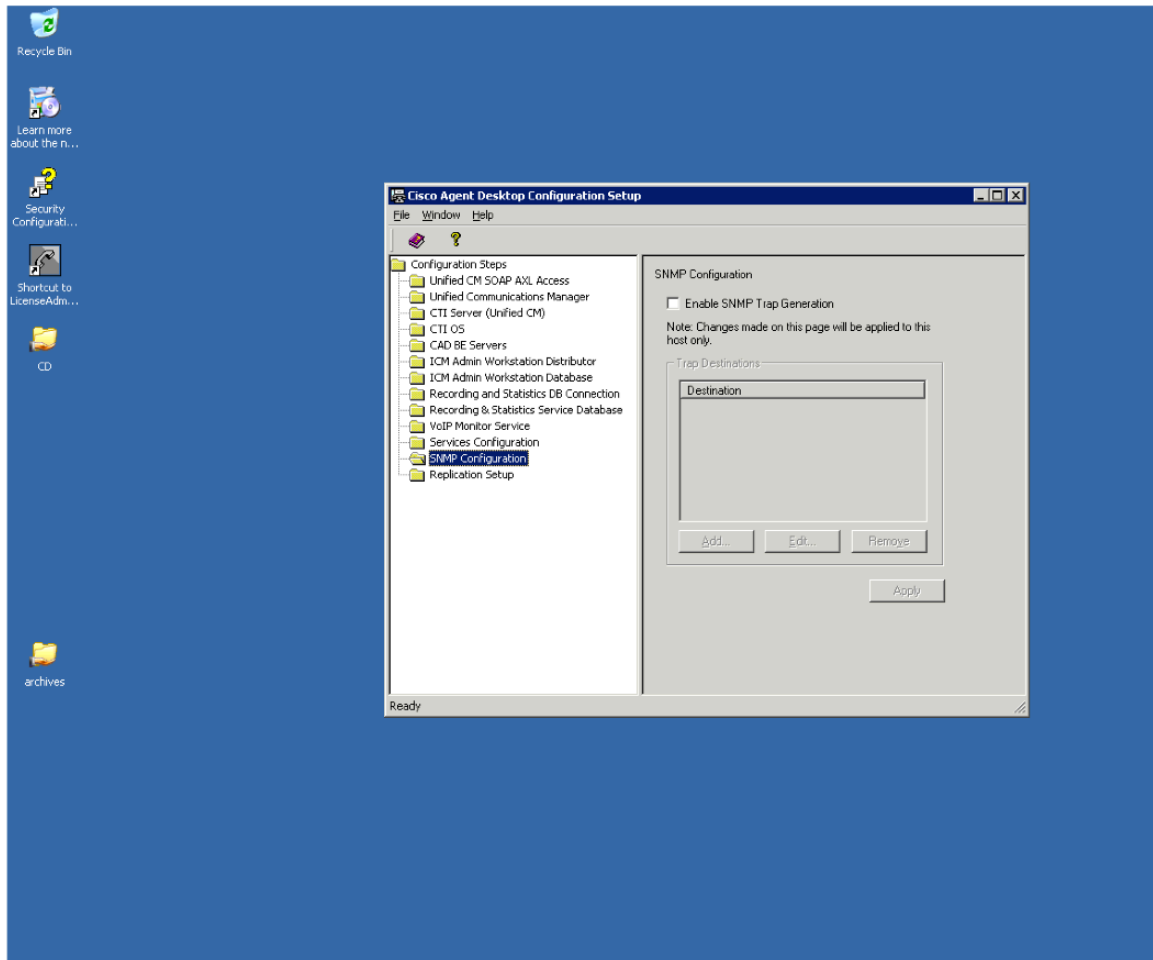
#### 8.1.14 SNMP Configuration

The SNMP Configuration step appears only if you are running the CAD Configuration Setup utility again to change configuration settings and if the Simple Network Management Protocol (SNMP) service is installed on the server that hosts the CAD base services.

SNMP allows you to monitor and manage a network from a single workstation or several workstations, called SNMP managers. SNMP is actually a family of specifications that provide a means for collecting network management data from the devices residing in a network. It also provides a method for those devices to report any problems they are experiencing to the management station.

When CAD is not running on a PG, configure the Microsoft SNMP service. When CAD is running on a PG, Cisco SNMP Agent Management service must be enabled and the Microsoft SNMP service must be disabled. The Microsoft SNMP service and the Cisco SNMP Agent Management service cannot simultaneously be enabled.

If you select the Enable SNMP Trap Generation check box, INFO and higher error messages are sent from the CAD services server to the IP addresses configured in the Destination pane. Use the Add, Edit, and Remove buttons to manage the list of destination IP addresses.



### 8.1.15 Thin Client Environment

This node will only appear if you are running the CAD Configuration Setup utility on the PC where the thin client service is hosted.

If this installation of CAD is installed in a thin client environment (for example, Microsoft Terminal Services, Citrix, or VMWare), click Yes. If not, click No.

### 8.1.16 Replication Setup

The Replication node only appears when you run the CAD Configuration Setup utility again to change your settings.

Use this step to add a secondary Directory Services, a secondary Recording and Statistics service, or both, after initial system setup. The primary service then replicates data on the secondary service so that they contain identical information.

Before proceeding, ensure that both servers are up and services are turned on. If you are using SQL Server database, both SQL instances must be on and the firewalls must be properly configured.

**NOTE:** If you have chosen a flat file implementation, Directory Services Replication is on by default and the Recording and Statistics Replication option is not displayed.

To set up Directory Services replication, select On for Directory Services Replication. Enter the primary and secondary server IP addresses in the fields, and then click Apply.

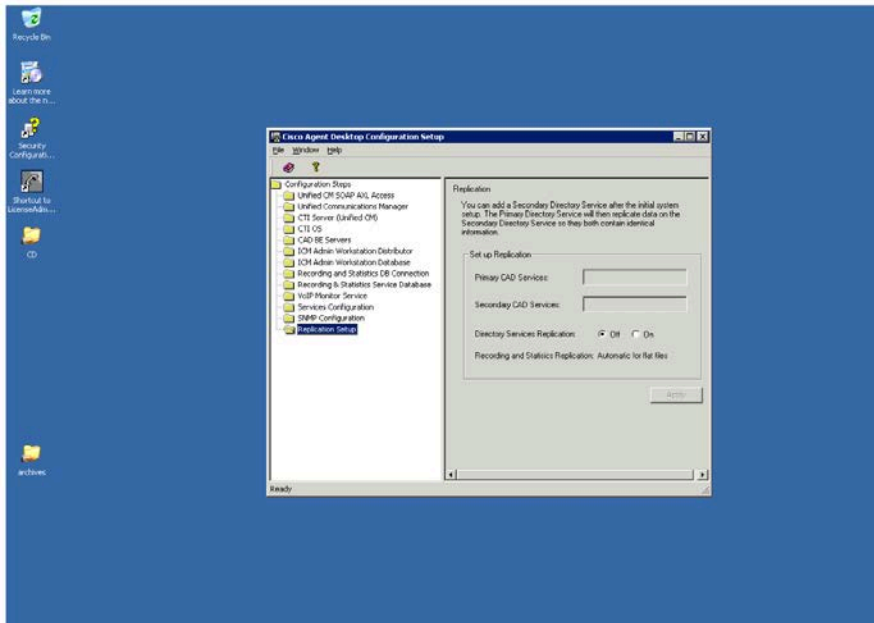
### Configuring a Secondary Server in a Replicated System

Complete the following procedure if you are running the CAD Configuration Setup utility for the first time on the secondary server in a replicated system (Side B).

To enter configuration data on the secondary base services computer (Side B):

1. The CAD Configuration Setup utility starts automatically and displays the Location of the CAD Base Services dialog.
2. Enter the IP address of the primary CAD base services and then click OK. A dialog box appears asking if you want to set up Directory Services replication.
3. Click Yes. The Secondary CAD Base Services dialog appears.
4. Enter the IP address of the server that hosts the secondary CAD base services, and then click OK. A confirmation dialog box appears prompting you to indicate whether the primary and secondary IP addresses are correct.
5. Click Yes to set up replication. When replication is done, the CAD Configuration Setup utility launches.
6. The fields for each node are already populated based on the information entered with the CAD Configuration Setup utility on the primary server (SideA). Navigate through the nodes and verify that the information is correct.
7. When you have reviewed all nodes, click Save on the toolbar or choose File > Save. When the data is successfully saved, the program ends automatically.

**NOTE:** The save process might take several minutes.



### 8.1.17 Modifying Configuration Settings

You can run the CAD Configuration Setup utility again to change your configuration settings.

To modify CAD configuration settings:

1. Start the CAD Configuration Setup utility using one of the following methods:
  - In Desktop Work Flow Administrator, select the logical contact center node in the left pane and then choose Setup > Configure Systems from the menu bar.
  - On another CAD host computer, navigate to the folder ...\\ProgramFiles\\Cisco\\Desktop\\bin and double-click postinstall.exe. The CAD Configuration Setup utility starts and displays the Location of the CAD Base services dialog
2. Verify that the primary and secondary IP addresses for CAD base services are correct, then click OK. The CAD Configuration Setup utility launches.

The nodes will appear in the following order:

- a. Unified CM SOAP AXL Access
- b. Unified Communications Manager
- c. CTI Server (Unified CM)
- d. CTI OS
- e. CAD-BE Servers
- f. ICM Admin Workstation Distributor
- g. ICM Admin Workstation Database
- h. Recording and Statistics Database Configuration
- i. Recording and Statistics Service Database
- j. VoIP Monitor Service
- k. Services Configuration

## I. Replication

**NOTE:** To switch between the left and right pane, press F6. To move up and down the left pane, use the up and down arrows.

3. Select the node you want to modify from the left pane, enter the new data in the right pane, and then click Apply
  - You can access the nodes in any order.
  - If you modify something in a node, you must click Apply to save your changes before you move on to another node.
4. When you are done making your changes choose File > Exit or click Close. The CAD Configuration Setup utility closes.
5. Restart the CAD base services and all desktops for your changes to take effect.

## 8.2 Licensing CAD 9.0

After you have installed and configured CAD, Unified CCE License Administration automatically starts. You can license your software at this point or close the application and license your software later. Your CAD software will not run until you have licensed your CAD services. You can re-run Unified CCE License Administration whenever you want to update the number of seats you have purchased.

Current licenses persist when upgrades are made on existing or new servers. No new licenses are required.

**NOTE:** Licensing your software can only be completed by a Cisco channel partner or Cisco Professional Services.

### 8.2.1 Obtaining a License Account

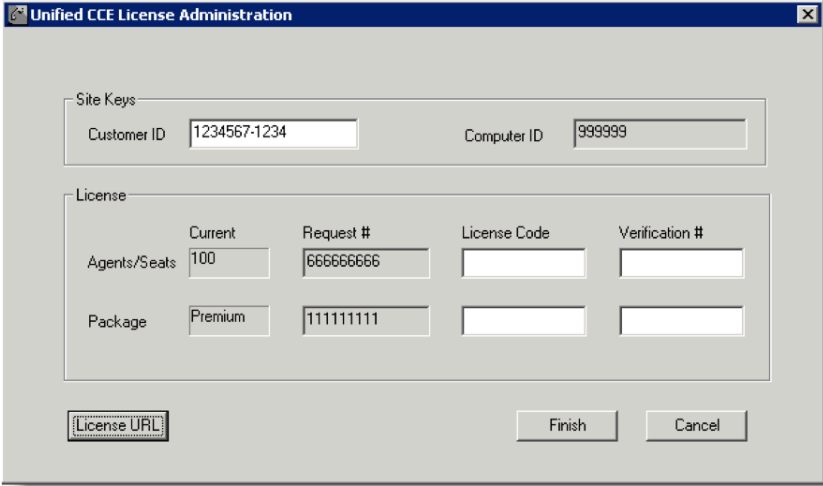
You must obtain a license account user ID and password to license your software. To obtain a license account:

1. Open Internet Explorer.
2. Navigate to the following address:  
<http://cadlicensing.com/sws/WebLicensingInitial/InitialLicensePage.html>
3. Click the Create a License Account hyperlink.
4. Complete the Partner License Request Form, then click E-mail Request. After your request is processed, your user ID and password will be e-mailed to you.

### 8.2.2 Using Unified CCE License Administration

To license CAD 9.0:

1. Launch LicenseAdmin.exe, in the folder ...\\Program Files\\Cisco\\Desktop\\bin. Unified CCE License Administration appears.
2. Click License URL. Internet Explorer is launched and accesses the website at  
<http://cadlicensing.com/sws/ciscoLicense/LicenseRegister.html>



The image shows a 'Unified CCE License Administration' dialog box. It has two main sections: 'Site Keys' and 'License'. The 'Site Keys' section contains two text boxes: 'Customer ID' with the value '1234567-1234' and 'Computer ID' with the value '999999'. The 'License' section contains two rows of data. The first row is for 'Agents/Seats' with a 'Current' value of '100', a 'Request #' of '66666666', and empty 'License Code' and 'Verification #' boxes. The second row is for 'Package' with a 'Current' value of 'Premium', a 'Request #' of '11111111', and empty 'License Code' and 'Verification #' boxes. At the bottom, there is a 'License URL' button, and 'Finish' and 'Cancel' buttons.

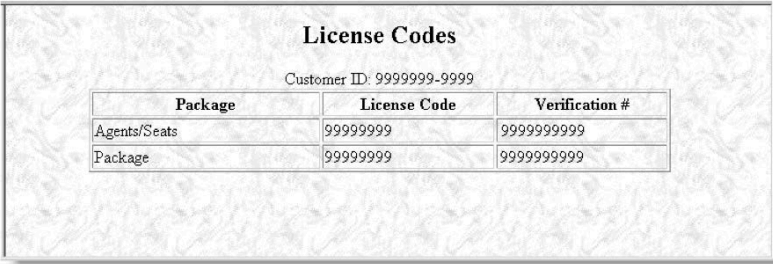
Site Keys	
Customer ID	1234567-1234
Computer ID	999999

License				
	Current	Request #	License Code	Verification #
Agents/Seats	100	66666666		
Package	Premium	11111111		

Buttons: License URL, Finish, Cancel

- Follow the instructions on the website. All of the information is required.
- Click Submit. The website displays a page listing the license codes and verification numbers you need to license your product.



The image shows a 'License Codes' page. It has a title 'License Codes' and a subtitle 'Customer ID: 9999999-9999'. Below this is a table with three columns: 'Package', 'License Code', and 'Verification #'. The table has two rows: 'Agents/Seats' and 'Package'. Both rows have the same values for 'License Code' and 'Verification #': '99999999'.

License Codes		
Customer ID: 9999999-9999		
Package	License Code	Verification #
Agents/Seats	99999999	9999999999
Package	99999999	9999999999

- Enter the Customer ID, License Codes, and Verification numbers in Unified CCE License Administration, and then click Finish. All of the licensed applications are activated.

### 8.3 Component Checkpoint

Use CTIOS toolkit to login an agent and verify that the agent login is successful and that the agent is able to move from Not Ready to Ready state as desired.

## 9 Cisco Agent Desktop Client Configuration

---

### 9.1 CAD client installation

CAD dynamically creates its installation and maintenance release packages for the agent, supervisor, and administrator desktop client applications during the course of installing or upgrading the CAD base services on the host (typically a peripheral gateway). The resulting CAD MSI packages are located on the production server in this location:

C:\Program Files(x86) \Cisco\Desktop\Tomcat\webapps\TUP\CAD.

The MSI files stored in this folder are intended for use in both manual and automated deployments. The benefit of creating the install packages within the context of the server-side installation is that the resulting client MSIs include deployment-specific information (such as server host IP address and language selection) that facilitate a silent client-side installation.

#### 9.1.1 Installing Desktop Administrator

1. From the desktop on which you want to install Desktop Administrator, access the following URL, where <CAD\_server> is the IP address of the server on which the CAD base services are installed.  
[http://CAD\\_server:8088/TUP/CAD/Admin.html](http://CAD_server:8088/TUP/CAD/Admin.html)  
The Desktop Administrator installation web page appears.
2. Follow the instructions on the web page to install the application.

#### 9.1.2 Installing Agent Desktop and Supervisor Desktop

1. From the desktop on which you want to install Agent Desktop or Supervisor Desktop, access the following URL, where <CAD\_server> is the IP address of the server on which the CAD base services are installed:  
[http://CAD\\_server:8088/TUP/CAD/Install.htm](http://CAD_server:8088/TUP/CAD/Install.htm)  
The Agent Desktop, Supervisor Desktop, and Agent Desktop—Browser Edition
2. Installation web page appears.
3. Follow the instructions on the web page to install the selected application.

#### 9.1.3 Installation Notes

- When you install Supervisor Desktop, Agent Desktop is installed automatically. Both applications are needed for a supervisor to use all the functionality of Supervisor Desktop.
- If you attempt to install Supervisor Desktop on a computer that already hosts Agent Desktop, you will receive error messages that a conflicting application has been detected. You must first uninstall Agent Desktop to avoid this.

#### 9.1.4 To reconfigure CAD client installation programs:

1. Run the CAD Configuration Setup utility on the CAD base services server.
2. From the menu, choose File > Reset Client Installs. This process reconfigures the client installation programs.

3. When the process is complete, the message, “Client installs reset” is displayed. Click OK to close the message. You can now install the client applications from the installation web pages.

## 9.2 Workflow Administrator

Both UCCX and UCCE use Cisco Agent Desktop and hence the following configuration is same for both UCCX & UCCE based Remote-Expert Solution.

With Cisco Agent Desktop, enterprises can integrate telephony data with data processing applications without modifying the existing applications. To deliver this compelling benefit, Cisco Agent Desktop uses workflows-powerful tools that automate agent activities. Voice contact workflows automate agent activity based on telephony and ACD events such as ringing, answered calls, dropped calls, and call wrap-up codes.

Workflows follow an event -> rule -> action behavior paradigm that is straightforward, yet the results are powerful. An event is a contact center activity that corresponds to a real-world state transition, such as the ringing of the phone at an agent's position, a change in an agent's ACD state, or time of day. For each event, sets of rules are evaluated to determine what actions to perform based on the rules for that event. A set of actions is defined for each set of rules, and this action set defines the integration of the telephony data with the desktop application and the execution of that desktop application. Figure below shows an example of workflow.

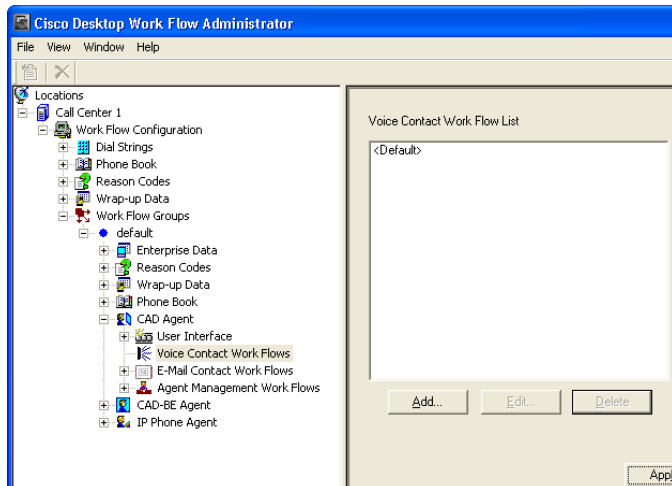


Cisco Agent Desktop Web Integration Action links to Web-based applications.

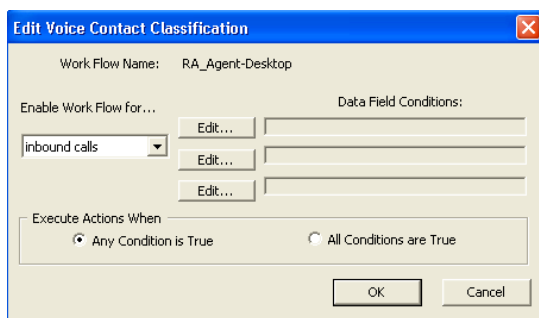
There are three events used for UCCX CAD integration with RESC – Ringing, Answered & Dropped. Open Cisco Agent Desktop Admin application and follow these steps.

1. Select Voice Contact Work Flows as shown below. Select ‘Voice Contact Work Flow’ from CAD agent sub-menu of CAD Admin.

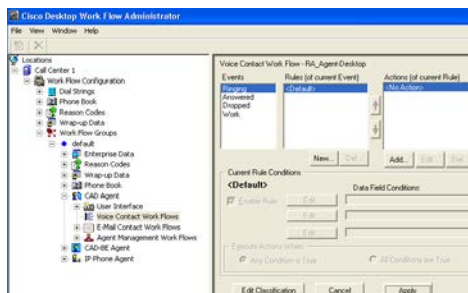




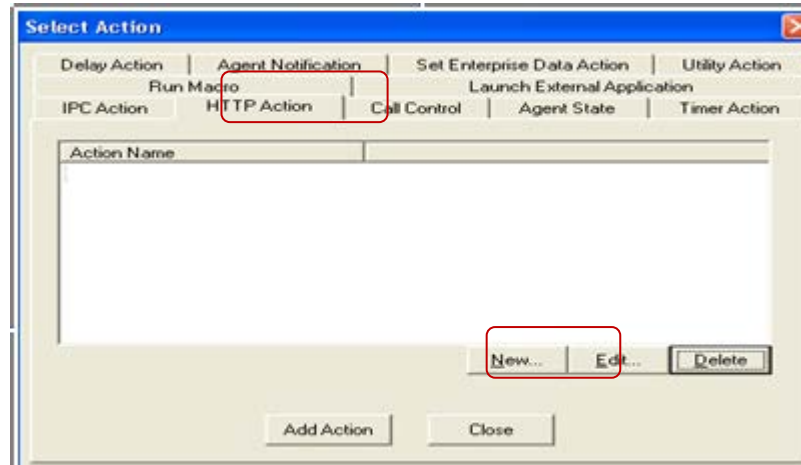
2. Select 'Add' from the Voice Contact Work Flow List on the right window.
3. Use a name (e.g. RA\_Agent\_Desktop) and press OK
4. Select the default value and press OK.



5. Select 'Ringing' event and select 'Add' from the 'Actions (of current rule)'



6. A 'Select Action' popup is seen



7. Now add the 5 actions from the table listed below, into the 'Select Action' popup.

#	Field	Value
1.	Action Type	HTTP Action
	Action Name	Ringing
	Protocol	http
	Method	GET
	Host	REM_IP
	Port	80
	Path	read/html/kiosk.jsp
	Request Data	
	Value Name	agent
	Value Type	Datafield
	Value	[Agent_ID]
	Value Name	calling
	Value Type	Datafield
	Value	Calling#

<b>2.</b>	Action Type	HTTP Action
	Action Name	Answered
	Protocol	http
	Method	GET
	Host	REM_IP
	Port	80
	Path	read/html/kiosk.jsp
	Request Data	
	Value Name	agent
	Value Type	Datafield
	Value	[Agent_ID]
<b>3.</b>	Action Type	HTTP Action
	Action Name	disconnect
	Protocol	http
	Method	GET
	Host	REM_IP
	Port	80
	Path	read/html/common.jsp
	Request Data	
	Value Name	agent
	Value Type	Datafield
	Value	[Agent_ID]
	Value Name	request

Value Type	UserDefined
Value	disconnected
<b>4.</b> Action Type	Launch External Application
Action Name	DCInvoke
Application	..CSI\DirectConnect\bin\DirectConnect\DirectConnect.exe
Arguments	[AGENT_ID]
<b>5.</b> Action Type	Launch External Application
Action Name	DCExit
Application	..CSI\DirectConnect\bin\DirectConnect\DirectConnectClose.exe
Arguments	None
<b>6.</b> Action Type	HTTP Action
Action Name	Not Ready
Protocol	http
Method	GET
Host	REM_IP
Port	80
Path	read/html/common.jsp
Request Data	
Value Name	agent
Value Type	Datafield

Value	[Agent_ID]
Value Name	state
Value Type	UserDefined
Value	1
<b>6. Action Type</b>	HTTP Action
Action Name	Ready
Protocol	http
Method	GET
Host	REM_IP
Port	80
Path	read/html/common.jsp
Request Data	
Value Name	agent
Value Type	Datafield
Value	[Agent_ID]
Value Name	state
Value Type	UserDefined
Value	0

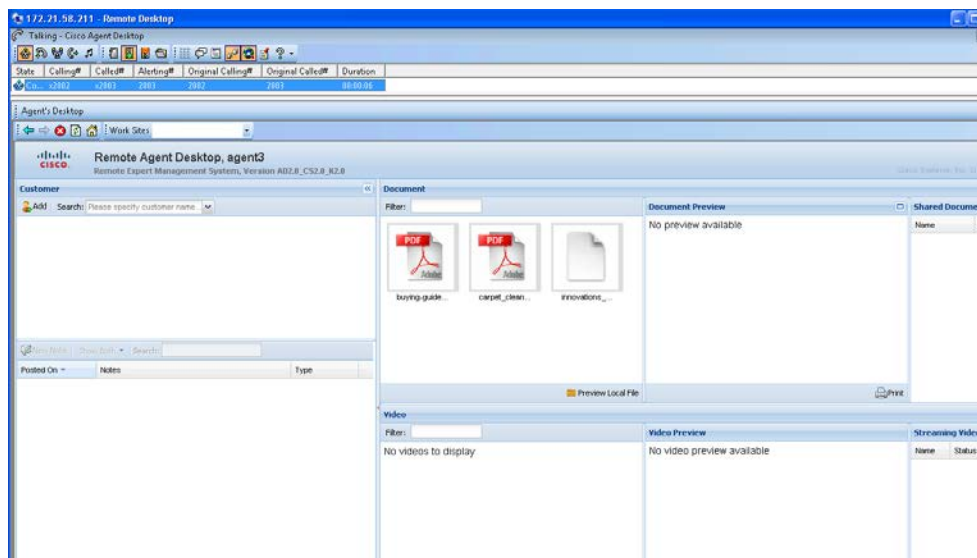
8. Associate the Events to the actions as seen in the table below. In order to associate an event, select the even from the **left** Events panel and then select the relevant action from the **right** Actions panel (while the specific event is still selected).

Event	Action
Ringing	DCInvoke, Ringing
Answered	Answered
Dropped	DCExit, disconnect

**Note** Please note that the path field is case sensitive 'read/html/kiosk.jsp'. Change the IP address of the host to the actual IP address of the RESC Virtual Machine, which is hosting the Kiosk App.

9. Apply and save the new changes and exit from this workflow.
10. Navigate to the Agent Management Work Flows
11. Click on **Ready** under Events in the left window panel and add the **Ready** action in the right panel.
12. Click on **Not Ready** event in the left window panel and add the **Not Ready** action in the right panel.
13. Apply and save the changes.

When agent login to their respective Cisco Agent Desktop (CAD), they will inherit the new rule. For example, after this new rule is applied, when the expert receives 'Ringing' on their phone, it will bring up an integrated browser based Agent Application window within the CAD as shown below.



### 9.3 Component Checkpoint

- Use Admin App “personnel” function to verify configured agents show up properly
- Verify agents can log into CAD and see the READ populated.

## 10 VXML Gateway Configuration

---

Voice Extensible Markup Language (VXML) is a standard defined by the World Wide Web Consortium (W3C). VXML is designed to create audio dialogs that provide synthesized speech, recognition of spoken words, recognition of DTMF digits and recordings of spoken audio. The VXML server and clients use the well-known HTTP protocol to exchange VXML documents and pages.

Cisco Voice Portal (CVP) delivers intelligent and interactive voice response (IVR) applications that can be accessed over the phone. There are three types of CVP deployments:

- Standalone Service
- CVP Call Control
- Call Queue and Transfer

Synthesized speech, recognition of spoken words or DTMF digit functionalities are provided by Text-to-Speech (TTS) and Automatic Speech Recognition (ASR) servers. Cisco IOS® VXML Gateway communicates with the TTS and ASR servers using Media Resource Control protocol (MRCP). There are two versions of MRCP (RFC 4463), namely MRCPv1 (MRCP over RTSP) and MRCPv2 (MRCP over SIP).

In this section we will do a high level walk through the vxml configuration pertaining to the Remote Expert Smart Solution.

### 10.1 IOS Configuration

Lets dive straight into the configuration. As we go by and encounter Remote Expert specific or affecting configurations, they will be highlighted with **text**

Current configuration : 8702 bytes

!

! No configuration change since last restart

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname vxm1gw43

boot-start-marker

```
boot system flash:c3900-universalk9-mz.SPA.152-2.T1.bin
```

```
boot-end-marker
```

```
!
```

```
card type command needed for slot/vwic-slot 1/1
```

```
logging buffered 51200 warnings
```

```
enable password cisco
```

```
!
```

```
no aaa new-model
```

```
no network-clock-participate slot 1
```

```
!
```

```
no ipv6 cef
```

```
!
```

```
ip domain name re18lab.com
```

```
ip cef
```

```
multilink bundle-name authenticated
```

```
!
```

```
crypto pki token default removal timeout 0
```

```
!
```

```
crypto pki trustpoint TP-self-signed-3307930257
```

```
enrollment selfsigned
```

```
subject-name cn=IOS-Self-Signed-Certificate-3307930257
```

```
revocation-check none
```

```
rsakeypair TP-self-signed-3307930257
```

```
!
```

```
!
```

```
crypto pki certificate chain TP-self-signed-3307930257
```



certificate self-signed 01

```

3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 33333037 39333032 3537301E 170D3132 30363230 30313034
34375A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 33303739
33303235 3730819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100AC71 9BFC1B9E 778E4A06 08E32B95 3BB42256 A97EFB06 FA2D8D46 9D8EC230
E4CEF353 87B31655 C9D56E55 7D7B1DAE 222FF49A B8A5D445 F64B7915 7B368773
109F79F4 B1BFDAAF C5C8FEB1 156E7E0E 9BC900E0 DF9B98D9 92E68D02 5B907B71
674926C4 3BBB186C 7AF519A0 C3DF8829 90ADF027 64B082C5 EEB85A97 9F1C0539
6BDD0203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603
551D2304 18301680 14BFD315 4350B54C 1FB247B2 3EAE0A1E 0938BE7F FB301D06
03551D0E 04160414 BFD31543 50B54C1F B247B23E AEE0A1E0 938BE7FB 300D0609
2A864886 F70D0101 05050003 81810088 86A19E17 E5361E41 46F90835 BB32E993
137CA799 22313E31 D066088D 81E0FB32 DBB50235 F3D8EBB4 F2B00D04 36C53276
F9BEF066 6F4A6B20 9B366182 CA7E13F6 F8CD8728 28BFAFDB 4233B892 92413539
C4743CF8 93A1E394 FD36B4C1 015A2E8E 707CDB75 FF756056 AC20FF93 7EDC353F
BFC3DE24 E1FA2473 10564EA8 E063D0

```

quit

voice-card 0

dspfarm

dsp services dspfarm

!

voice-card 1

!

```
!  
voice call send-alert  
voice rtp send-recv  
!  
voice service voip  
ip address trusted list  
ipv4 192.168.71.31  
!-- IP address of CVP server  
allow-connections h323 to h323  
allow-connections h323 to sip  
allow-connections sip to h323  
allow-connections sip to sip  
signaling forward unconditional  
fax protocol t38 version 0 ls-redundancy 0 hs-redundancy 0 fallback none  
sip  
rel1xx disable  
min-se 1200 session-expires 1200  
header-passing  
options-ping 60  
!-- forces early offer  
early-offer forced  
voice class codec 1  
!-- requirement for Remote Expert solution.  
codec preference 1 g711ulaw  
!  
http client cache memory pool 15000
```

http client cache memory file 1000

http client cache refresh 864000

!--- Define the amount of maximum memory to use for downloaded prompts.

ivr prompt memory 15000

!

!--- Configure an application service for CVP VXML CVPSelfServiceBootstrap.vxml.

application

service new-call flash:bootstrap.vxml

!

service cvp-survivability flash: survivability.tcl

!

service CVPSelfService flash:CVPSelfServiceBootstrap.vxml

!

service ringtone flash:ringtone.tcl

!

service cvperror flash:cvperror.tcl

!

service handoff flash:handoff.tcl

!

service bootstrap flash:bootstrap.tcl

!

!

!--- Specify the maximum memory size for the HTTP Client Cache.

http client cache memory pool 15000

!--- Specify the maximum number of file that can be stored in the HTTP Client Cache.

http client cache memory file 500

!--- Disable Persistent HTTP Connections.

no http client connection persistent

!

rtsp client timeout message 10

mrtp client timeout connect 10

mrtp client timeout message 10

mrtp client rtpsetup enable

vxml tree memory 500

vxml audioerror

vxml version 2.0

license udi pid C3900-SPE150/K9 sn FOC161769JB

hw-module pvdm 0/0

!

hw-module sm 1

!

ip http server

ip http access-class 23

ip http authentication local

ip http secure-server

ip http timeout-policy idle 60 life 86400 requests 10000

!

ip route 0.0.0.0 0.0.0.0 192.168.71.1

!

```
access-list 23 permit 10.10.10.0 0.0.0.7

dialer-list 1 protocol ip permit

!

nls resp-timeout 1

cpd cr-id 1

!

snmp-server community public RO

snmp-server enable traps entity-sensor threshold

!

control-plane

!

!

mgcp profile default

!

sccp local GigabitEthernet0/0

sccp ccm 192.168.71.40 identifier 1 version 7.0

sccp

!

dial-peer voice 1 pots

description CVP TDM dial-peer

service cvp-survivability

incoming called-number .T

direct-inward-dial

!

!--- Dial-peer used to play ring tone to the customer

dial-peer voice 919191 voip
```

```
description CVP SIP ringtone dial-peer

service ringtone

incoming called-number 9191T

voice-class codec 1

voice-class sip rel1xx disable

dtmf-relay rtp-nte h245-signal h245-alphanumeric

no vad

!

!-- Dial-peer used to play error tone to the customer

dial-peer voice 929292 voip

description CVP SIP error dial-peer

service cvperror

incoming called-number 9292T

voice-class codec 1

voice-class sip rel1xx disable

dtmf-relay rtp-nte h245-signal h245-alphanumeric

no vad

!

!

!-- Dial-peer used to queue the call

dial-peer voice 1234569 voip

description Used for VRU leg

service bootstrap

incoming called-number 123456T

voice-class codec 1

dtmf-relay rtp-nte h245-signal h245-alphanumeric
```

```
no vad

!

!

gateway

media-inactivity-criteria all

timer receive-rtp 1200

!

sip-ua

retry invite 2

retry bye 1

timers expires 60000

timers connect 1000

reason-header override

!

!
```

## 10.2 Component Checkpoint: Verify VXML GW operation

Ensure the vxmlgw services are configured and the dial-peers are in place.

Consider reducing voice file cache time during setup/testing.

### 10.2.1 Show commands

**show call active voice brief**

**show mrp client session active detail**

**show voip rtp connections**

**show http client cache**

### 10.2.2 Debug Commands

Configure the IOS Gateway to log the debugs in its logging buffer and disable-logging console.

Note: Refer to [Important Information on Debug Commands](#) before you use **debug** commands.

These are the commands used to configure the Gateway in order to store the debugs in the Gateway's logging buffer:

- service timestamps debug datetime msec
- service sequence
- no logging console
- logging buffered 5000000 debug
- clear log
- debug isdn q931
- debug voip ccapi inout
- debug voip application vxml default
- debug voip application vxml dump
- debug rtsp all
- debug mrcp all
- debug http client all
- debug voip rtp session nte named-event



## 11 Customer Voice Portal Server Configuration

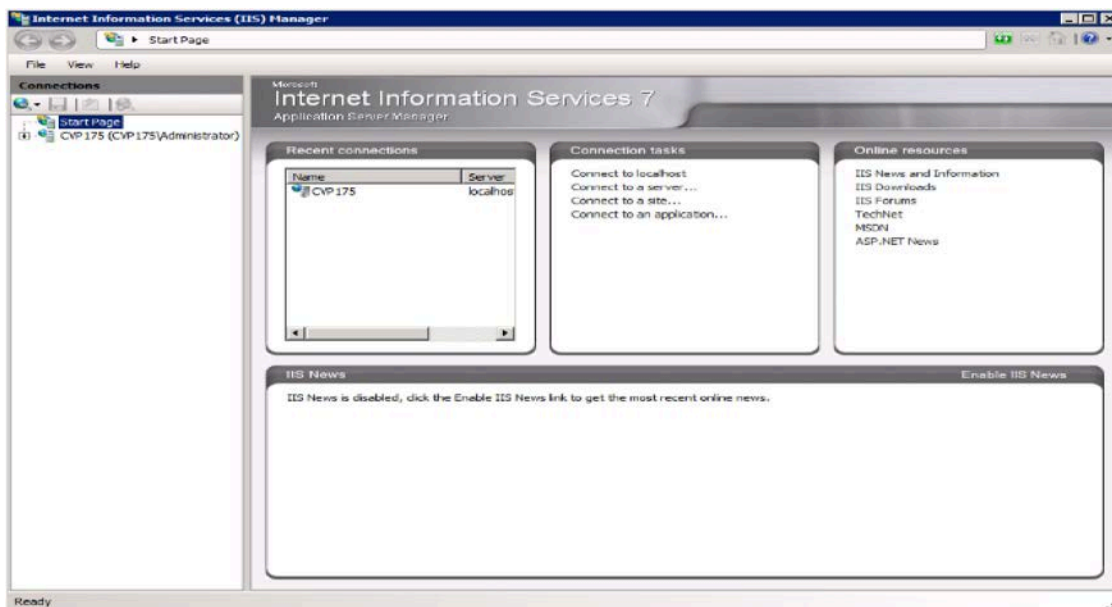
Unified CVP components can be deployed using the single OVA on any CVP supported virtualization hardware. Virtualization of the following deployments and Unified CVP components on Cisco Unified Communications Systems (UCS) hardware is supported:

- Unified CVP Call/Media Server
- Unified CVP VXML Server
- Unified CVP Reporting Server
- Unified CVP Ops Console

For the **Remote Expert** solution, we would require only the CVP Call/Media Server and CVP OAMP (Ops Console) specifically. We proceed through this document assuming the CVP Call Server and CVP OAMP server are installed based on the guidance from the [CVP 9.0 Installation Guide](#). The sections that follow focus on the configurations associated with setting up CVP for the Remote Expert smart solution.

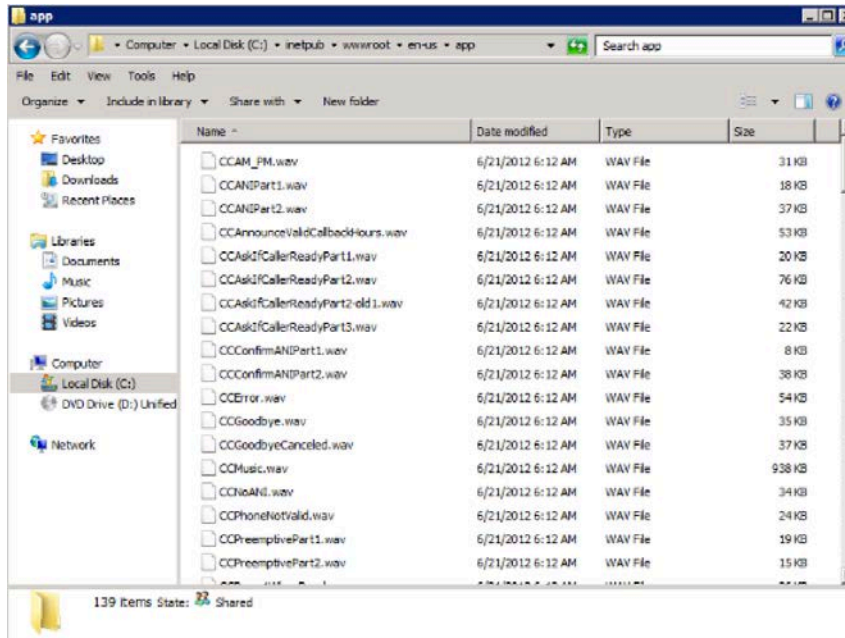
### 11.1 CVP Media Server Configuration

This setup uses Microsoft IIS as the web server to host the media files.

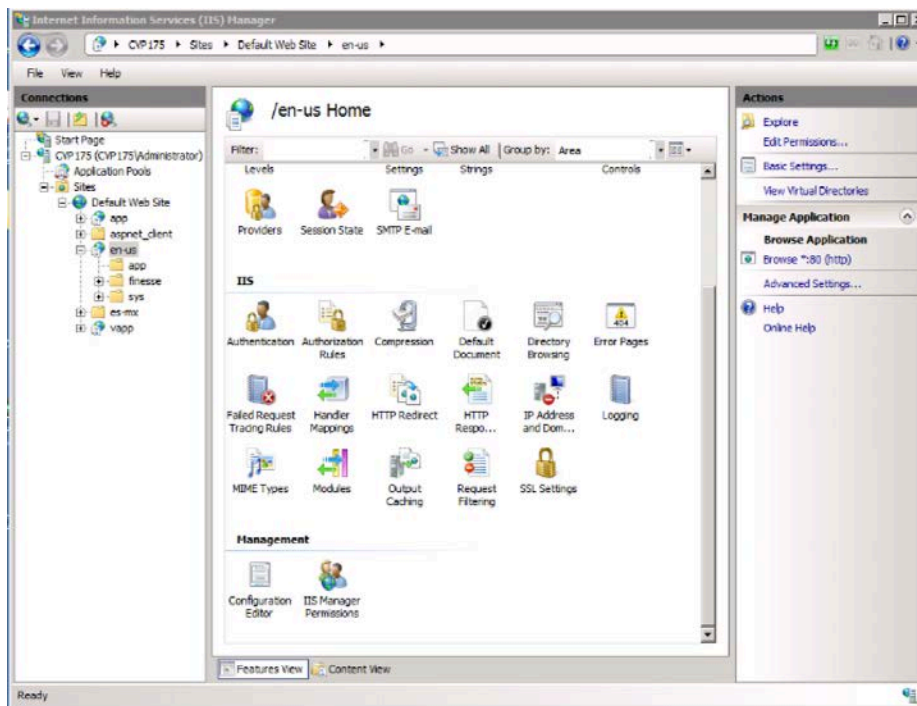


## Quick Steps

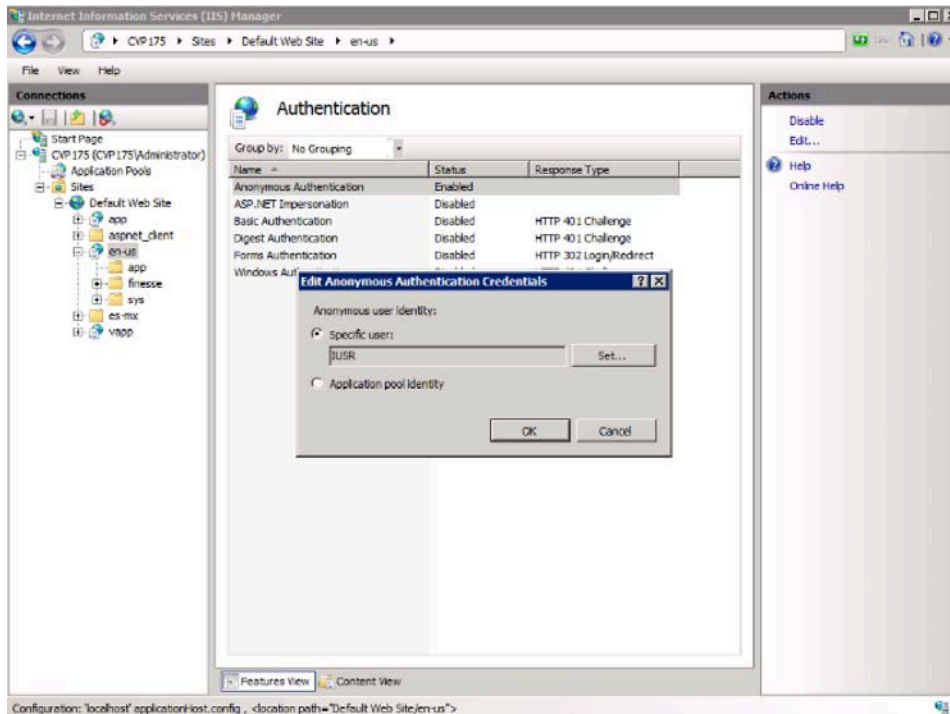
1. The CVP installation places some basic media files in the IIS web server path C:\inetpub\wwwroot\en-us\app.



2. Either create a Virtual Directory linking to the Media Files installed by the CVP setup.exe in the above path, or link to the "en-us" folder in the root of the IIS Web server.



3. Make sure anonymous access is enabled and the built-in IIS User is assigned.



4. Create a folder named Custom below the en-us folder if you would like to place your custom media files in a new location. In our case we would need to place the silence.wav file on the media server in a desired location.
5. Apply configuration changes and save.
6. Restart IIS

We need to ensure to point to the silence.wav file in the ICM script (the audio to be played to the endpoint when placed in queue) and you should be able to access this file from any compatible browser using for example [http://cvp\\_server/en-us/app/silence.wav](http://cvp_server/en-us/app/silence.wav).

## 11.2 CVP Configuration

Before configuring CVP call server, it should be important to know little bit about the setup and SIP call flows.

High Level CVP call flow overview	
CUCCE Pilot Number	IP Phone caller dials CTI route point number 3333
Routing Client	SIP Gateway is the routing client

Label Returned to SIP GW by ICM	123456789+cid
Processing at CVP	CVP Call Server send this label 123456789+cid to VXML-GW
Processing at VXML-GW	VXML-GW has an incoming dial-peer configured that basically invokes the bootstrap tcl service
Processing at VXML-GW	Now a sequence of VXML communications happens between the VXML GW and CVP IVR Service. This communication is called MicroApps.
Processing at CVP	At this point CVP sends the same label 123456789+cid to ICM to inform that VXML-GW resources are engaged
Queue music	ICM instructs CVP to play custom music to the endpoint based on the script configuration.

Once you understand the high level overview of the call flow, it will be easy to understand the static routes needed by the CVP Call Server.

### 11.2.1 CVP Operations Console

Unified CVP provides Voice over IP (VoIP) routing services for the Cisco Unified Intelligent Contact Management Enterprise (Unified ICME) and Cisco Unified Contact Center Express (UCCX) products. Unified ICME provides the services necessary to determine where calls should be routed, whether to ACDs, specific agents, or to VRUs, but the routing services themselves must be provided by an external routing client.

A typical deployment of the Unified CVP solution requires operating, administering, managing and provisioning multiple servers and IOS components. The **Operations Console** is a web-based console that enables users to centrally operate, administer, maintain and provision the Unified CVP solution.

We would be adding the CVP Call server and the VXML GW information and other CVP configuration using the CVP Operations Console or the CVP OAMP platform.

### 11.2.2 CVP Call Server

CVP call server talks to the VRU pim that was earlier configured as part of the ICM setup. The VRU pim exists on the Peripheral Gateway of the ICM and it enables routing messages between CUCM and ICM in addition to serving as a media server to play back ICD prompts.

Steps:

1. Login to CVP Operations console as administrator
2. Proceed to Device Management -> Unified CVP Call Server
3. Click on Add New.
4. Provide the CVP Call server IP Address and hostname. Also enable to ICM, IVR and SIP services. Ensure that the device version and build information displayed is correct.

The screenshot shows the 'Edit Unified CVP Call Server Configuration' page in the Cisco Unified Customer Voice Portal. The 'General' tab is selected, showing fields for IP Address (172.19.239.175), Hostname (CVP175), Description, and Device Version (CVP 9.0(1) Build=679). The 'Turn on Services' section shows ICM, IVR, and SIP services enabled. The 'Save' and 'Save & Deploy' buttons are at the bottom right.

5. You can choose to leave the ICM and IVR tabs with default configurations since it doesn't affect our RE call flow.
6. Proceed to SIP service tab. Here, if you are using DNS SRV to resolve server farm names or service names, please enable this option and select the DNS SRV server/outbound proxy host details that proceeds below.
7. Enter 91919191 in the 'DN on the gateway to play ringtone' and 92929292 for the 'DN on the gateway to play the error tone' fields unless you are planning to use a different DN in the vxml gateway configuration.
8. Save and Deploy.

The screenshot shows the 'Edit Unified CVP Call Server Configuration' page in the Cisco Unified Customer Voice Portal, with the 'SIP' tab selected. The 'Configuration' section includes options for 'Enable outbound proxy', 'Use DNS SRV type query', 'Resolve SRV records locally', 'Outbound proxy Host', 'Outbound SRV domain name/Server group name (FQDN)', 'DN on the Gateway to play the ringtone' (91919191), and 'DN on the Gateway to play the error tone' (92929292). The 'Local Static Routes' section shows static routes for local routing without an outbound proxy. The 'Save' and 'Save & Deploy' buttons are at the bottom right.

### 11.2.3 VXML Gateway

The vxml gateway configuration is added to the Operations console in order to identify and be able to communicate with the vxml gateway where the tcl services reside.

**Steps:**

1. Login to the CVP operations console as Administrator user.
2. Proceed to Device Management -> Gateway
3. Click on Add New.
4. Provision the correct vxml gateway IP Address, Hostname and Device Type.
5. On the right panel enter the correct credentials and port information (telnet/ssh) that is used to login to the gateway ios. Click on Test Sign-in to confirm the configuration.
6. Click on Save and deploy.

The screenshot shows the 'Edit Gateway Configuration' page in the Cisco Unified Customer Voice Portal. The page is divided into two main sections: 'General' and 'Username and Passwords'. The 'General' section contains fields for IP Address (172.19.239.177), Hostname (VXML-GW), Device Type (2900), Description, Trunk Group ID (300), and Location ID. The 'Username and Passwords' section contains fields for Username (cisco), User password, Enable password, and Port (23). A 'Test Sign-in' button is located next to the Port field. A 'Save' button is at the bottom right of the page.

Once this is complete proceed to Bulk Transfer -> File Transfer -> Scripts and Media. Select gateway from 'Select Device Type' and move the newly configured gateway from the Available frame to the Selected frame. Select 'Default Gateway files' from the Scripts and Media files box and click on Transfer. Confirm the status using the File Transfer Status button. This ensures that the right version of scripts and media files are placed on the vxml gateway by transferring those files from the CVP to the gateway using either ssh or telnet that was configured earlier.

Once this is complete, follow the steps in Quick Steps 1-6 to add CUBE as a gateway to the CVP Operations console.

### 11.2.4 CVP Media Server

The discussed earlier Media Server is the server on which the media files reside. It is a good practice to configure this server using the Operations Console.

**Steps:**

1. Login to the CVP operations console as Administrator user.
2. Proceed to Device Management -> Media Server
3. Click on Add New.
4. Provision the Media Server IP Address and Hostname details.

### 11.2.5 Dialed Number Pattern

This is where we configure the routing on the CVP. It is similar to using Route Patterns in the Cisco Unified Communications Manager if you are comfortable with the CUCM method.

## Steps:

1. Login to the CVP operations console as Administrator user.
2. Proceed to System -> Dialed Number Pattern
3. Click on Add New.
4. Enter the label returned by ICM for the given call flow as the Dialed Number Pattern. Use '>' as a wild card to correlate with 'X' used in CUCM.
5. Proceed to the Dialed Number Pattern Types and select 'Enable Local Static Route'
6. In the Route to Device, select the vxml gateway from the dropdown.
7. The IP Address, Host Name, Server group name gets auto populated.
8. Click on Save
9. Complete the configuration by clicking on Deploy. If Deploy is not clicked, the configuration doesn't take effect.

In a similar fashion complete the Dialed Number Pattern configurations using the table below as guidance.

Dialed Number	Route to Device
123456> (label returned by ICM)	VXML gateway
20> (Expert DN pool)	CUBE
9191>	VXML gateway
9292>	VXML gateway

### 11.2.6 Miscellaneous

Listed below are few things that might help with the configurations from a CVP point of view.

1. You need to upload licenses before starting the configurations. You can do this by logging into Operations console and proceeding to Bulk Transfer -> File Transfer -> License. Select the license(s) from the local system and upload them into the CVP setup.
2. Every configuration added into CVP needs to be saved and then Deployed. Ensure that you click the 'Deploy' button once confirmed.
3. If you are deploying a Highly Available setup, it is good practice to do it using DNS SRV records added to the common DNS Server in the infrastructure. However CVP also gives you an option to configure the records locally on the call server/operations console and this is provided in the Call Server SIP configuration screen.
4. You can also configure SIP Server groups for configuring redundant components, which go into the Device Configuration menu.
5. Notices that CVP call flows are valid for the Type 10 VRU only.
6. Observe that "cid" is actually the correlation ID and is a numerical value.
7. It's a good practice to take a backup once the configuration is complete. This can be done using System -> Expert System backup and entering a valid location to take the backup.

### **11.3 Solution Checkpoint: Verify Call Routing**

1. Check to confirm that on UCCE -> PG -> Diagnostic framework the VRU PIM is in Active state
2. Check to confirm that with ICM script in monitor mode, we see the call lodged at the RunExtScript node
3. Check that the silence or the configured media is being played back with no experts available/logged in
4. Dial pilot number from video endpoint to verify functionality



## 12 Remote Expert Manager Hardware Provisioning

In order to minimize the number of physical servers required when deploying the Remote Expert Smart Solution, best practice calls for installing REM and IEM as virtual machines (VMs) on a host platform running the VMWare hypervisor 5.x.

### 12.1 Host Provisioning For Virtual Deployments

Table 2 presents the recommended specifications for the physical host running the IEM and REM VMs.

Table 1 - Recommended Host Platform Specifications

Item	Description
Server platform	Cisco UCS C220 M3 server
Form factor	2 rack units (2RU)
Minimum requirements:	
Processor	2 x Intel Xeon processors E5-2650 at 2.00 GHz (8-core)
Cache	40 MB (20 MB per processor)
RAM	48 GB
Storage controller	RAID-capable
Hard disk	4 x 600-GB 10,000-rpm SAS
Power supply	2 x 650 watts (W)
Hypervisor	VMware ESXi 5

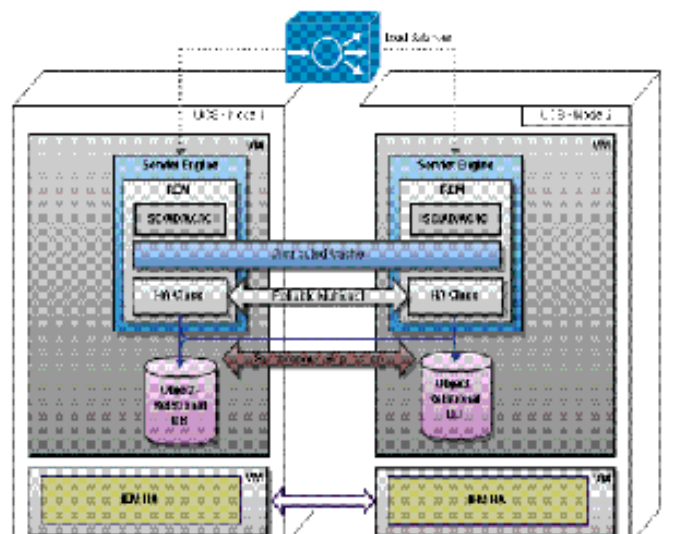
While best practice recommends installing IEM and REM on a dedicated physical host, this is not a strict requirement. However, as with any virtualized host environment, performance problems may occur if the physical host(s) do not scale to the required load. Please see the Cisco Remote Expert Manager Administration Guide for more information on benchmarking REM performance in a virtualized environment.

For deployments of more than 1000 customer pods, create additional Cisco IEM virtual machines as necessary. Note that there is no communication between the Cisco IEM instances, so the group of customer pods controlled by each Cisco IEM must be managed independently.

## 12.2 Host Platform Considerations for Remote Expert Manager High Availability

While Cisco Remote Expert Manager may be deployed in a stand-alone environment, best practice calls for deploying REM in a high-availability configuration.

Cisco REM achieves high availability of the services it offers by using hardware-based server load balancers such as the Cisco ACE Module, as well as component-level hardware and software application redundancy, as detailed in Figure n.



Implementing REM high availability requires deployment of a pair of redundant physical hosts as described in the previous section, with each hosting an identical Cisco REM/IEM environment. For more information on the REM high availability architecture, please see the **Cisco Validated Design for the Remote Expert Smart Solution 1.8. Installing and configuring REM in a standalone and redundant configurations is covered in Section 15.**

## 13 Interactive Experience Manager (IEM) Installation and Configuration

---

This chapter provides you with the information you need to install and configure the Cisco Interactive Experience Manager (IEM) for use with the Remote Expert Smart Solution, and includes the following sections:

- Install IEM Software
- Configure Server Settings
- IEM High Availability
- Component Checkpoint: Verify Installation and Initial Configuration

### 13.1 Install and Configure IEM Software

To install and configure the IEM, follow the instructions in Chapter 1 of the [Cisco Remote Expert Manager 1.8 Installation Guide](#).

### 13.2 IEM High Availability

To install IEM for High Availability, please refer to the [Cisco Interactive Experience Manager High Availability Installation and Configuration Guide](#).

### 13.3 Component Checkpoint: Verify Installation and Initial Configuration

After completing the procedures described in the previous sections, verify that you can successfully complete the following tasks:

- Use an ssh client to connect to the IEM command line/menu driven interface at the IEM's configured IP address and/or hostname without any error messages.
- Log into the IEM command line/menu driven interface using the "installer" account with a non-default password.
- Verify that the IEM server is synchronized to one or more NTP time sources, and that the correct time zone is set for the server's physical location.
- Verify that IEM is successfully licensed for use.
- Browse to the IEM Administration web page at the IEM's configured IP address and/or hostname without any browser or plug-in error messages.
- Log into the IEM Administration page using a non-default Account and Username credentials with Administrator privileges.
- Verify SMTP Provider Configuration.
- Verify remote logging configuration.
- SSL certificates and private keys are uploaded correctly (optional).
- Verify that one or more IEC-4600 policies exist as necessary to support the various physical Customer Pod locations where IEC-4600s will be installed.
- (Optional) Verify one or more IEC-4600s exist as managed devices in the IEM device collection.
- Verify Device Registration is enabled.

## 14 Interactive Experience Client (IEC) Provisioning and Configuration

---

This chapter provides you with the information you need to install and configure Cisco Interactive Experience Clients (IECs) for use with the Remote Expert Smart Solution, and includes the following sections:

- Deploy one or more Customer Pods featuring an IEC-4600 Series Client
- Component Checkpoint: Verify Installation and Initial Configuration

### 14.1 Deploy One or More Customer Pods Featuring an IEC-4600 Series Client

Please refer to Chapter 2 of the [Cisco Remote Expert Manager 1.8 Installation Guide](#) for the steps required to provision, install and configure an IEC-4600 series client within a Customer Pod for use with the Remote Expert Smart solution.

### 14.2 Component Checkpoint: Verify Installation and Initial Configuration

After completing the procedures described in the previous sections, verify that you can successfully complete the following tasks for the provisioned IEC-4600s:

- Log into the IEM Administration page.
- Verify that the endpoints are successfully registered with IEM.
- Verify that the endpoints are running at the correct firmware version

## 15 Remote Expert Manager Installation and Configuration

---

This chapter provides you with the information you need to install and configure the Cisco Remote Expert Manager (REM) for use with the Remote Expert Smart Solution, and includes the following sections:

- Install REM Software
- Configure Server Settings
- Deploy Default Branding Assets
- REM High Availability
- Component Checkpoint: Verify Installation and Initial Configuration

### 15.1 Install and Configure REM Software

To install the REM, follow the instructions in Chapter 3 of the [Cisco Remote Expert Manager 1.8 Installation Guide](#). This chapter also explains the steps required to configure REM for use with the Remote Expert Smart Solution.

### 15.2 Deploy Default Branding Assets

After initially configuring REM, please refer to Chapters C-D of the *Deploying the Cisco Remote Expert Manager for the Remote Expert Smart Solution 1.8 Guide* for the steps required to deploy the default set of branding assets, which are packaged as part of the Remote Expert Manager distribution. Best practices dictate installing and verifying basic operation of the solution using these “known good” assets before attempting to use the solution with assets created or provided by third parties.

### 15.3 REM High Availability

To install REM for High Availability, please refer to Chapter 3, Page 27 of the [Cisco Remote Expert Manager 1.8 Installation Guide](#).

### 15.4 Component Checkpoint: Verify Installation and Initial Configuration

After completing the procedures described in the previous sections, verify that you can successfully complete the following tasks:

- Use an ssh client to connect to the REM command line/menu driven interface at the REM’s configured IP address and/or hostname without any error messages.
- Log into the REM command line/menu driven interface using the “admin” account with a non-default password.
- Verify that the REM server is synchronized to one or more NTP time sources, and that the correct time zone is set for the server’s physical location.
- Verify that the rem.properties file is configured properly based on the requirements of the solution deployment (contact center selection, audio recording options, high-availability options, etc.)
- Verify that the CUCM and JTAPI user credentials are correctly configured.

- Browse to the REAC Administration web page at the REM's configured IP address and/or hostname without any browser or plug-in error messages.
- Log into the REAC Administration page using non-default credentials with Administrator privileges.
- Browse to **Error! Hyperlink reference not valid.** and click on the "Services" link to verify that all required services are running on the REM server.

## 15.5 Media Server Identification/Installation

REM requires an RTMP compliant media server or content distribution network for streaming video files to the Customer Pod. Once the Remote Expert Manager has been installed and verified operational, a suitable media server must be identified within the Customer's enterprise network and properly configured to interoperate with the Remote Expert Smart Solution.

Chapter 3 of the [Cisco Remote Expert Manager 1.8 Installation Guide](#) describes how to install a recommended media server if necessary.

## 15.6 Component Checkpoint: Verify Installation & Configuration of Media Server

If using a pre-existing, customer-provided media server with the Remote Expert Smart Solution, configuring and verifying media server operation is outside the scope of this document. However, interoperability of the media server with the Remote Expert Smart Solution can be verified during basic REM operational configuration, which is detailed in Chapter 15.1.

If a recommended media server from Chapter 3 of the [Cisco Remote Expert Manager 1.8 Installation Guide](#) is deployed, then proper operation of the media server may be verified by browsing to the IP address/hostname of the media server. A test video should play out in the lower half of the browser window.

## 16 Basic REM Operational Configuration Using the Remote Expert Administration Console (REAC)

Once REM is installed and initially configured, and you have either identified an existing media server or installed a media server for use with the Remote Expert solution, you can now begin to perform basic operation configuration. The goals of these basic configuration steps are to further verify that the infrastructure and applications installed to this point are operating correctly, and to prepare for the Solution Checkpoint where you will verify the basic operation of the entire solution.

### 16.1 Prerequisites

- (Optional) A production dial plan for the pilot numbers, agents and TelePresence endpoints participating in the Remote Expert Smart Solution
- A short on-hold video meeting the requirements of the Content Creation Guide (See Chapter 1 in [Cisco Remote Expert Manager 1.8 Administration Guide](#))
- A sample static graphic conforming to the standards in the Content Creation Guide to display on the TelePresence screen while the Customer Pod is idle.
- A sample document for sharing with the Customer Pod (such as a short PDF file)

### 16.2 Introducing REAC

You've already briefly experienced using the Remote Expert Administration Console (REAC) during initial installation and configuration of Remote Expert Manager. Detailed information about using REAC is available in Chapter 1 of the [Cisco Remote Expert Manager 1.8 Administration Guide](#). You will use that Guide to configure REM with enough information to verify the basic operation of the solution, using suggested example configuration parameters. For purposes of this verification, you may use the example parameters shown here, or similar parameters from your production environment if they are available.

Example Remote Expert Smart Solution Call Center Infrastructure		
Device	Locale	Directory Number
Customer Pod TelePresence Endpoint	N/A	X1001
Expert TelePresence Endpoint	N/A	X2001
Commercial Lending Pilot #	English	x3333
Home Mortgage Pilot #	English	x3333
Private Banking Pilot #	English	x3333
Problem Resolution Pilot #	English	x3333

Retirement Savings Pilot #	English	x3333
Small Business Pilot #	English	x3333
Help	English	x3333
Commercial Lending Pilot #	Spanish	X3333
Home Mortgage Pilot #	Spanish	x3333
Private Banking Pilot #	Spanish	x3333
Problem Resolution Pilot #	Spanish	x3333
Retirement Savings Pilot #	Spanish	x3333
Small Business Pilot #	Spanish	x3333
Help	Spanish	x3333

In this section, you will use the [Cisco Remote Expert Manager 1.8 Administration Guide](#) to complete the following tasks:

- Configure Locales
- Configure Expert Types and Pilot DNs for Skill Groups
- Configure Contact Center Agents as Remote Experts
- Upload and Designate Videos on Demand
- Upload and Designate Static Graphic Images for the Customer Pod
- Upload Documents for Sharing with the Customer Pod
- Create a Customer Feedback Survey
- Register Customer Pod with REM

### 16.2.1 Configure Locales

In order to verify basic functionality, configure a minimum of two locales, English and Spanish.

### 16.2.2 Configure Expert Types and Pilot DNs for Skill-Groups

Remote Expert Manager 1.8 allows you to create up to six expert types per locale. For purposes of verifying basic functionality, the example dial plan associates each skill type with the same pilot number. If the Unified Communications and Contact Center infrastructure for your deployment is already configured for production at this point, you may wish to use those pilot numbers instead.

### 16.2.3 Configure Contact Center Agents as Remote Experts

Depending on which contact center infrastructure was chosen for this deployment, the contact center agent user accounts may be created within CUCM, the contact center application, or both. Once these



agent user accounts are created, some or all of them may be designated as Experts participating in the Remote Expert Smart Solution.

For purposes of verifying basic functionality, the example dial plan lists one agent designated as an Expert. If the Contact Center infrastructure for your deployment is already configured for production at this point, you may wish to configure one or more agents instead.

Note that when specifying the “Expert UID” in REAC, be sure to use the agent’s “Login ID” for UCCE deployments and the agent’s “Login Name” for UCCX deployments.

#### **16.2.4 Upload and Designate Videos on Demand**

Cisco Remote Expert Manager requires uploading at least one video on demand file to stream to the Customer Pod when the agent places the Customer Pod TelePresence endpoint on hold. Use REAC to upload a suitable on-hold video and thumbnail image. You will test video streaming in a subsequent chapter of this document.

#### **16.2.5 Upload and Designate Static Graphic Images for the Customer Pod**

Use REAC to upload a suitable static graphic to display on the collaboration panel when the Customer Pod is idle.

#### **16.2.6 Upload and Documents for Sharing with the Customer Pod**

Use REAC to upload a document for sharing with the Customer Pod.

#### **16.2.7 Create a Customer Feedback Survey**

Use REAC to create a short feedback survey for each locale. If Spanish-language questions/responses are not available, just be sure to use a different set of questions/responses for the Spanish locale in order to distinguish the surveys from each other.

#### **16.2.8 Register Customer Pod with REM**

Use REAC to register at least one Customer Pod with REM using the example dial plan. If the Contact Center infrastructure for your deployment is already configured for production at this point, you may wish to refer to the production dial plan instead.

### **16.3 Component Checkpoint: Verify REM Operational Configuration**

Verify that each designated Expert agent is registered with REM, indicated by a green check box. If any Expert agent is not properly registered:

- Verify the Expert information entered in REAC matches the agent information configured in CUCM and/or UCCE.
- Verify that the REAC Expert UID is the agent’s “Login ID” for UCCE deployments or the agent’s “Login Name” for UCCX deployments.
- Verify the JTAPI user credentials configured in rem.properties match those configured in CUCM.

You will verify other aspects of the REM Operational Configuration during the Solution Checkpoint in Chapter 18.



The screenshot shows the Cisco Remote Expert Solution Administration Console. The top navigation bar includes the Cisco logo, the title "Remote Expert Solution Administration Console", and user information "admin" with "Log Out" and "About" links. A secondary navigation bar contains tabs: "Locale", "Expert Type", "Expert" (selected), "Video", "Content", "Document", "Kiosk", "Session", "DB Cluster", "LongPen", "Feedback", and "Mar". Below the navigation bar, the "Experts" section is displayed. It includes a toolbar with "Add", "Modify", "Delete", and "Refresh Registrations" buttons. A table lists the experts, with columns for "Expert Name", "Directory Number", "Expert User-Id", and "Registration Status". One expert, "Agent\_A", is listed with a directory number of "2001" and a user ID of "0001". The "Registration Status" for "Agent\_A" is indicated by a green checkmark, which is highlighted by a red rectangular box.

Expert Name	Directory Number	Expert User-Id	Registration Status
Agent_A	2001	0001	✓

## 17 DirectConnect Installation and Configuration and Integration with Cisco Agent Desktop (CAD)

---

This chapter provides you with the information you need to install and configure Direct Connect at the Expert workstation, allowing document sharing with the Customer Pod, and includes the following sections:

- Install Direct Connect Software
- Configure Direct Connect Settings
- Component Checkpoint: Verify Installation and Initial Configuration

### 17.1 Install and Configure Direct Connect Software

To install Direct Connect, follow the instructions in Chapter 3, Page 22 of the [Cisco Remote Expert Manager 1.8 Installation Guide](#). After you have installed Direct Connect, configure it for use with the Remote Expert Smart Solution by following steps in the same chapter.

### 17.2 Component Checkpoint: Verify Direct Connect Configuration

Verify that the `cv_service_url` in the `DirectConnect.exe.conf` file reflects the IP address or hostname of the REM server.

Verify that the Direct Connect server has been restarted to properly reflect configuration changes during installation.

You will verify the proper operation of Direct Connect during the Solution Checkpoint in Chapter 18.

## 18 Solution Checkpoint: Verify Basic System Functionality

---

This chapter provides the steps for verifying basic functionality of the Remote Expert Smart Solution. After verifying basic solution functionality, the solution is ready for further customization and acceptance testing based on the requirements of your specific deployment. This chapter includes the following sections:

### 18.1 Prerequisites

Meet the requirements and/or complete the steps in Chapters 2 through 17 of this document and ensure the following:

- Customer Pod registered with Remote Expert Manager
- Agent workstation configured for use with the Remote Expert Smart Solution
- Agent Workstation with an application to share with the Customer Pod (such as Adobe PDF Reader) and a suitable document for sharing
- Agent account registered as an Expert with Remote Expert Manager that is available for testing the solution

### 18.2 Log into Cisco Agent Desktop as a Remote Expert

In order to prepare for initiating a Remote Expert session:

1. Log in to Cisco Agent Desktop (CAD) using the credentials of an agent configured as a Remote Expert
2. No other Remote Expert agents should be logged in at this time
3. Once the agent is completely logged in to CAD, the agent should be in the “Not Ready” state. The browser portion of the agent’s desktop should look like this:



4. For now, leave the agent in the “Not Ready” state



## 18.3 Initiate a Remote Expert Collaboration Session via the Collaboration Panel

At this point, the Customer Pod should be idle and displaying a “home” screen on the Collaboration Panel, similar to the illustration below. In Chapter 16, you mapped one or more of the buttons shown on the Collaboration Panel to a contact center queue serviced by the Remote Expert agent that’s currently logged in to the call center.

Touch one of these buttons on the Collaboration Panel to initiate a Remote Expert session.

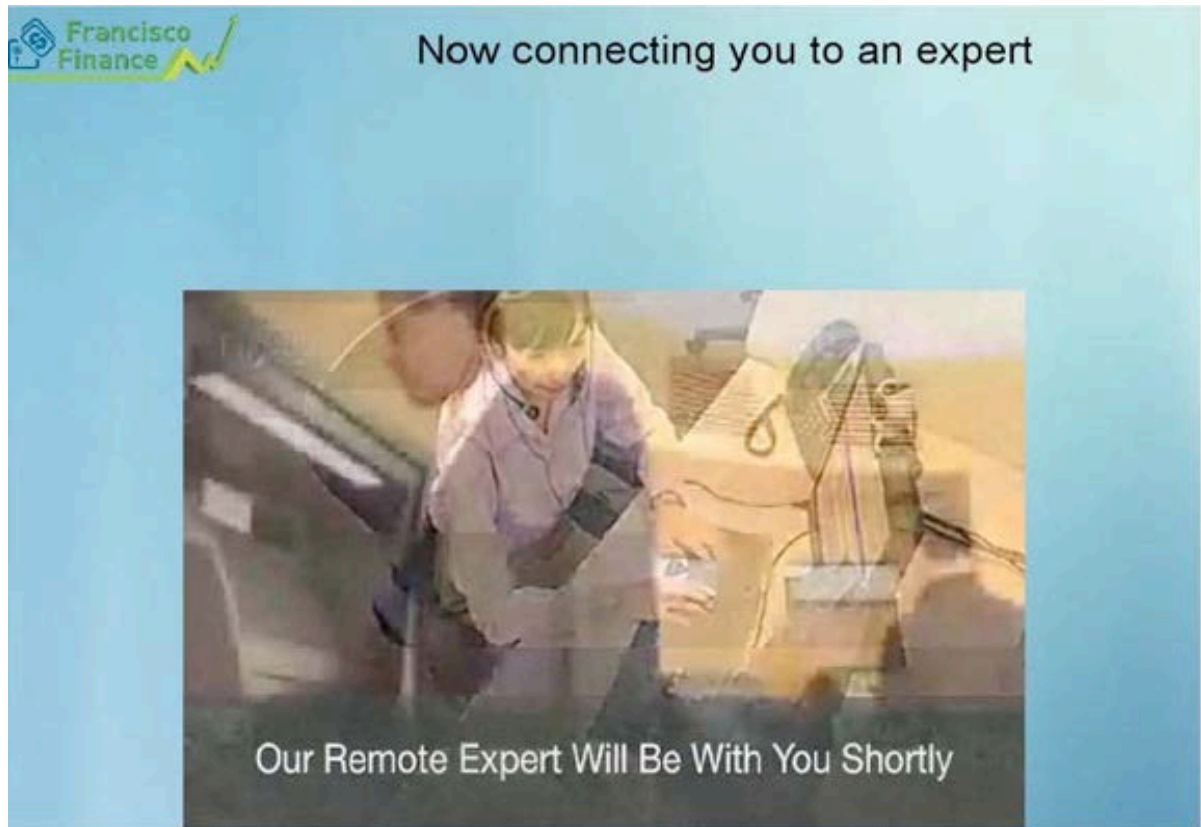
### 18.3.1 Expected TelePresence Endpoint Behavior While the Session is In Queue

1. Since the only Remote Expert logged into the call center is currently not ready, the session will initially be placed into queue
2. Depending on how the Contact Center is configured, the TelePresence endpoint in the Customer Pod may or may not play out a message announcing the call is being queued, hold music, etc.
3. Check with your contact center administrator to determine the correct behavior of the TelePresence endpoint while the call is in queue

4. This behavior should continue until the Remote Expert answers the call, or the session is terminated at the Customer Pod by hitting the “Cancel” button on the Collaboration Panel

### 18.3.2 Expected Collaboration Panel Behavior While the Session is In Queue

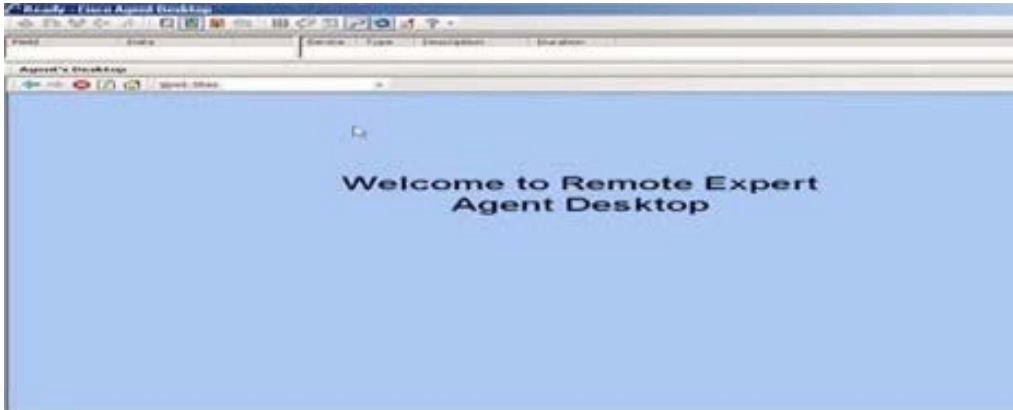
While the call is in queue, the Collaboration Panel should display a call progress screen and play a “Wait” audio and video clip, similar to the one shown below:



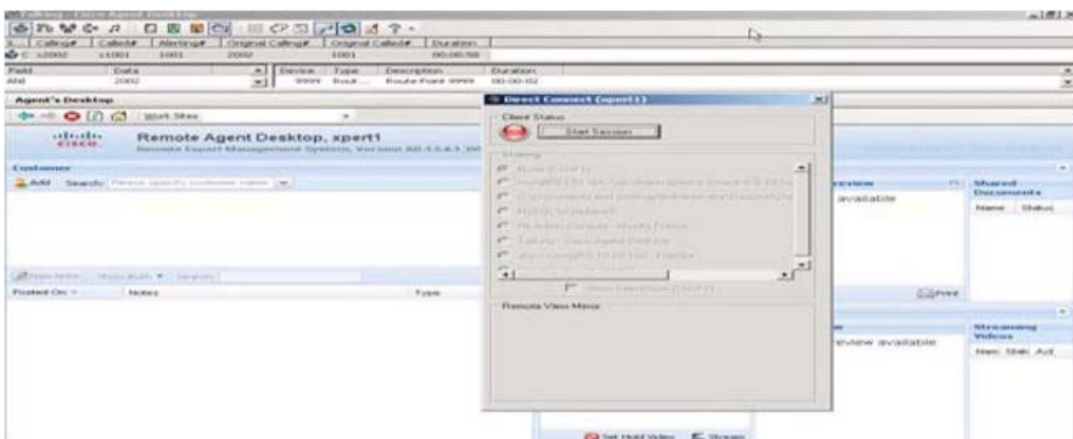
This behavior should continue until the Remote Expert answers the call, or the session is terminated at the Customer Pod by hitting the “Cancel” button on the Collaboration Panel.

### 18.4 Ready the Remote Expert, Answer an Incoming Call and Start a Remote Expert Session

1. Once the session is initiated from the Customer Pod, move the Remote Expert agent to the “Ready” state within CAD. The browser window of the agent’s desktop should now look similar to the screen shown below:



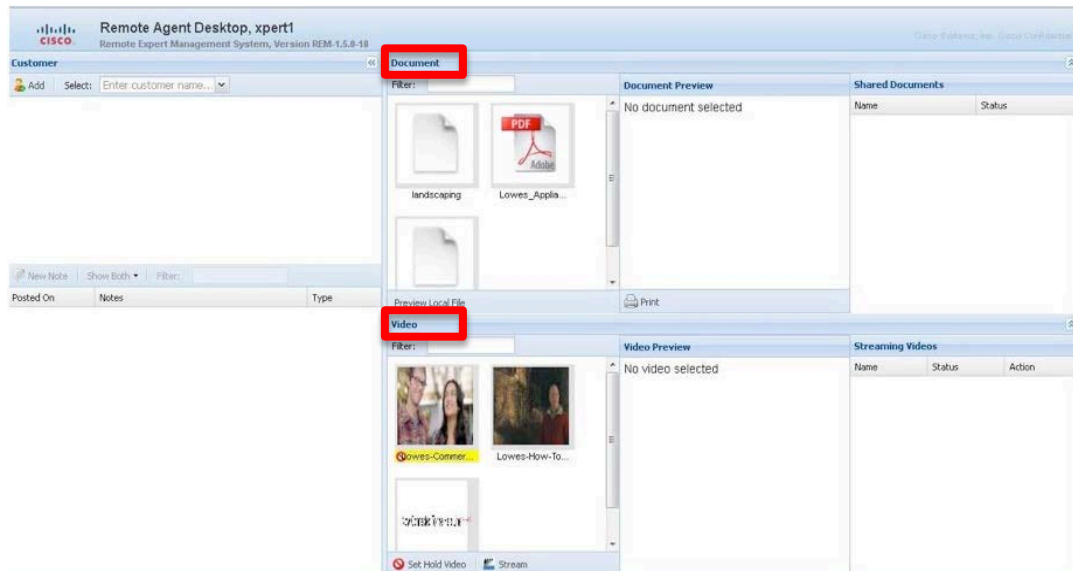
2. The Remote Expert agent's TelePresence endpoint should begin ringing once the contact center application acknowledges that an agent with the correct skill set is now available to answer the call
3. Once the Remote Expert agent answers the call, the agent's desktop should now look similar to the screen below:



4. The agent workflow configured for this agent should also start the Direct Connect application on the agent's workstation, as shown in the screen above
5. You may need to move or minimize the Direct Connect window in order to access certain parts of the Remote Expert Agent Desktop (READ). You will test the Direct Connect application later in this chapter
6. Ensure that the quality of the TelePresence call between the Expert and Customer Pod is as expected before moving on to test the features of READ

## 18.5 Verify READ Video and Document Inventory

In Chapter 16 you uploaded sample video and document assets to REM. Verify these video and document assets appear in READ in the "Video" and "Document" panes, respectively.



## 18.6 Preview and Share a Video with the Customer Pod

1. Select the video you uploaded in the READ Video pane
2. The video preview player should appear in the READ Video Preview pane
3. Click the Play button on the player and ensure that the video plays out correctly and completely in the Video Preview window
4. While the video is still selected in the Video pane, click the Stream button at the bottom of the Video pane
5. The Streaming Videos pane should indicate that the video is streaming
6. The Video should begin to play at the Customer Pod on the Collaboration Panel

## 18.7 Preview and Print Documents at the Customer Pod

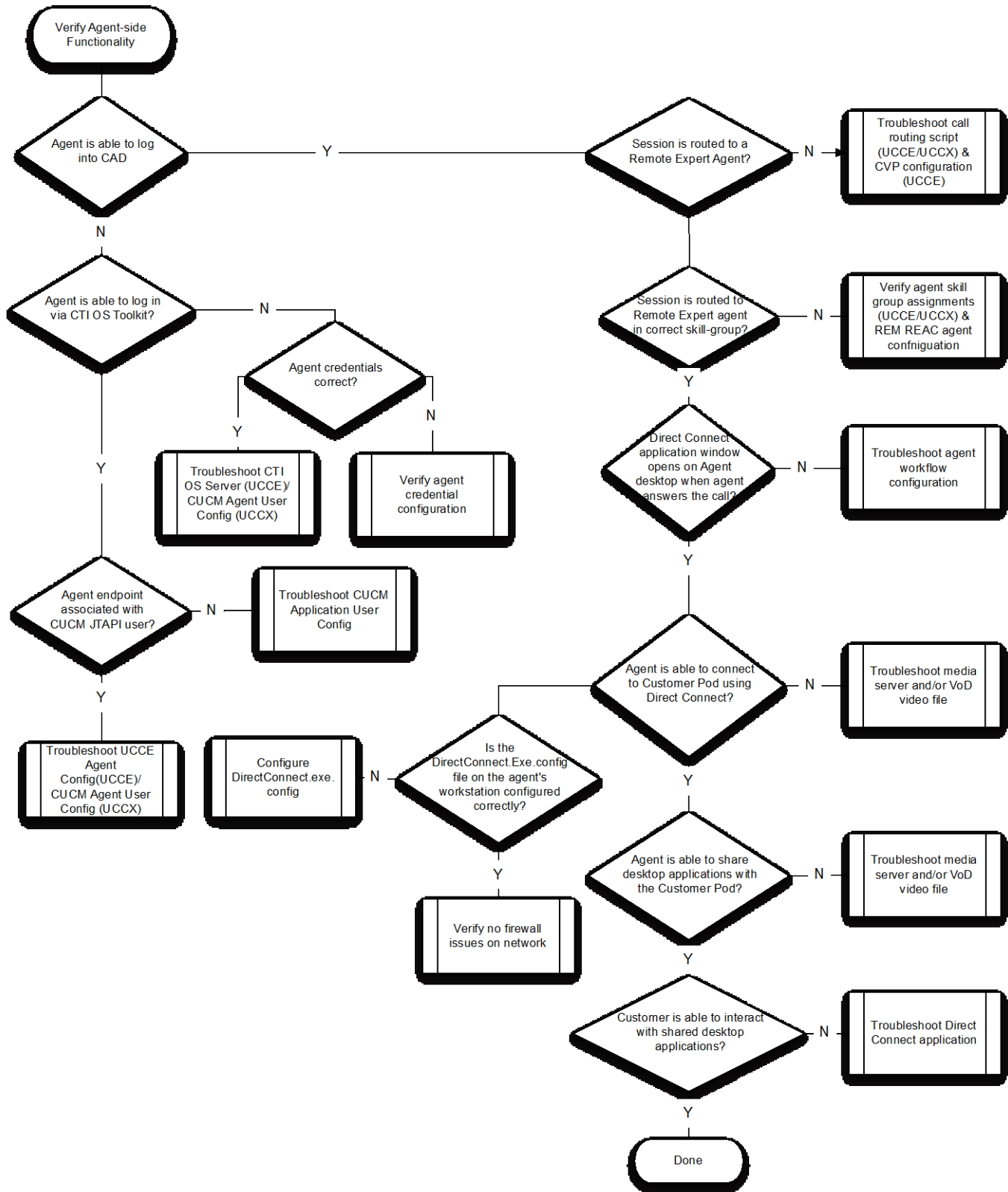
1. Select the document you uploaded in the READ Document pane.
2. The document preview should appear in the READ Document Preview pane
3. Ensure that the document appears correctly in the preview pane
4. While the video is still selected in the Document pane, click the Print button at the bottom of the Shared Documents pane
5. The Shared Documents pane should indicate the document status as initially in the print queue, followed by "Printed"
6. The document should print on the printer at the Customer Pod

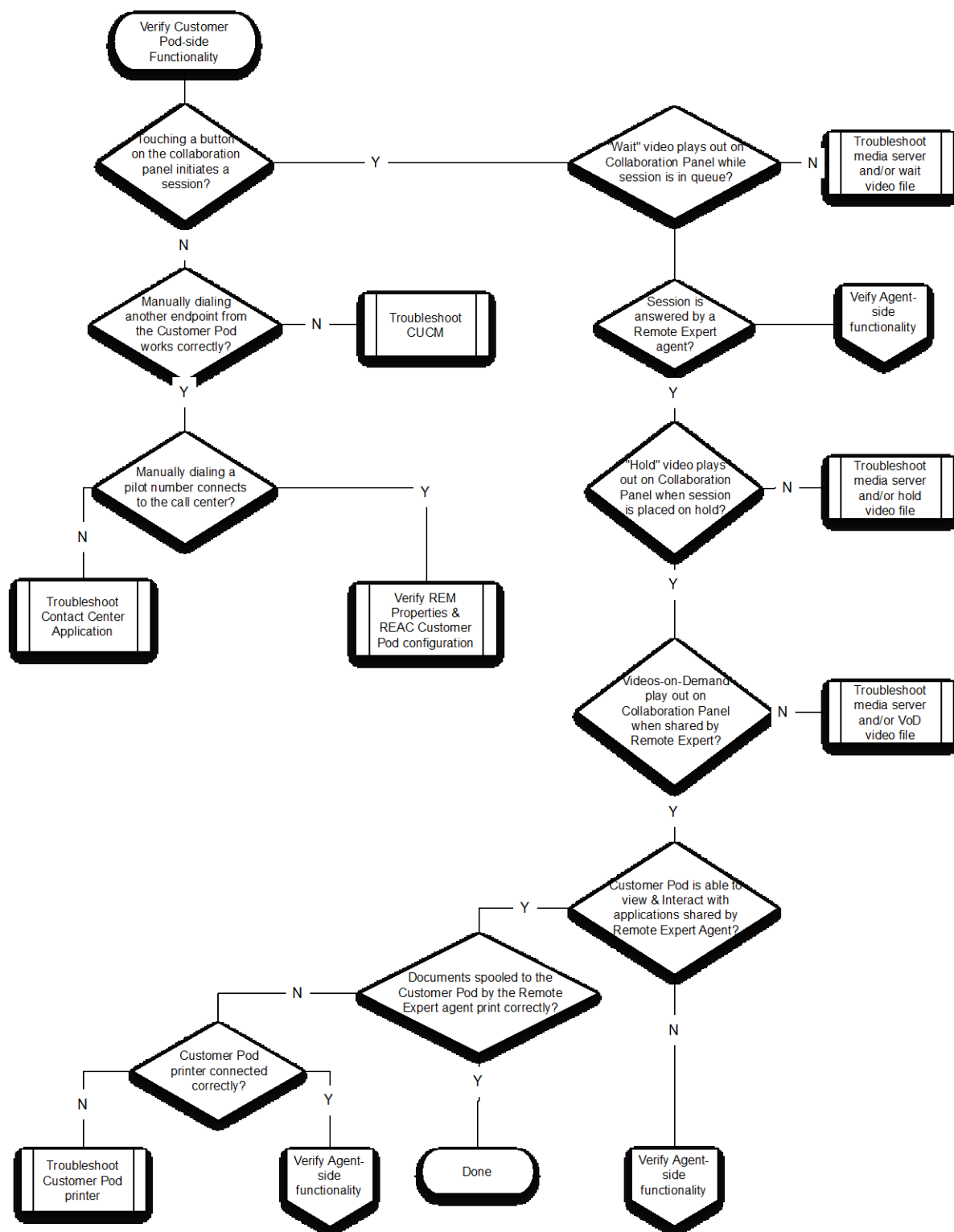
## 18.8 Use Direct Connect to Share an Application on the Agent Desktop with the Customer Pod

1. If you previously minimized the Direct Connect window to use READ, re-open the Direct Connect window
2. On the agent workstation, open an application to share with the customer pod
3. Open and preview a document within the application you are about to share
4. In the Direct Connect window, click the "Connect" button to establish a connection to the Customer Pod



5. Within a few seconds, the indicator in the Direct Connect window should change from red to yellow to green, and the “Connect” button will change to read “Disconnect” as the session is established
6. In the Direct Connect window, select the radio button for the application you wish to share with the Customer Pod
7. On the agent workstation, click the mouse within the window of the application to be shared to ensure that it is in focus. A green border will appear around the application when it is in focus with regard to Direct Connect, and a red border will appear when it is not in focus
8. The shared application window from the agent workstation should now appear at the Customer Pod on the Collaboration Panel
9. On the agent workstation, check the “Allow Interaction” box
10. At the Customer Pod, you should be able to interact with the shared application using the touch screen interface of the Collaboration Panel
11. On the agent workstation, in the Direct Connect window, click the “Disconnect” button to disconnect the Direct Connect sharing session
12. End the Remote Expert session by disconnecting the call from the CAD desktop. The Remote Expert session and TelePresence call should terminate
13. The CAD desktop should revert to the “Ready” state. The Direct Connect application on the agent workstation should terminate
14. At the Customer Pod, the Collaboration Panel should display the option for the Customer to complete a survey. Complete the survey
15. Ensure that the answers to the customer survey are displayed correctly in REAC.





## 19 Advanced Features

---

The previous chapters presented a step-by-step guide to deploying the “basic” features and functionality of the Remote Expert Smart Solution. In addition to these basic features, the solution supports a number of advanced features, including:

- Recording of the audio portion of the Remote Expert session
- Supervised transfer of a Remote Expert session between Remote Expert agents
- Supervised conferencing between the Customer Pod and up to two Remote Expert Agents
- Specialized Customer Pod peripheral integration

Information on the basic deployment of these features is found in the remaining chapters of this document. However, implementing certain features requires prerequisites, including:

- Integrating Cisco Unified Border Element (CUBE) with the Remote Expert Smart Solution
- Configuring MediaSense audio recording for the Remote Expert Smart Solution
- Integrating the Cisco Media Conferencing Unit (MCU) 4501 with the Remote Expert Smart Solution.

These prerequisites are covered in the following sections.

### 19.1 MediaSense

Cisco MediaSense records conversations on the network rather than on a device. This simplifies the architecture, lowers costs, provides optimum scalability, and facilitates use by analytics applications from Cisco technology partners.

In the Remote Expert solution, the MediaSense server is positioned to begin recording when the Customer is removed from the queue and connected to an Expert or a Contact Center Agent. This is done by CUBE initially forking the call to MediaSense so that for every conversation you have a stream being sent to the MediaSense server for recording purpose.

Here below we will cover some steps to setup MediaSense for basic audio recording the Remote Expert call flow.

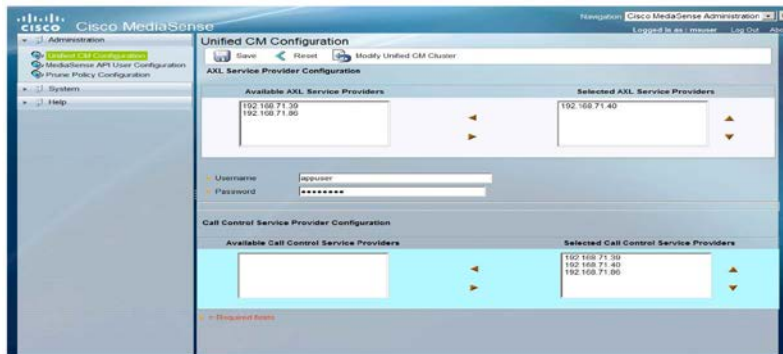
#### 19.1.1 CUCM Configuration

The MediaSense server needs to communicate with the CUCM for passing on the API and status information mainly useful for reporting.

Steps:

1. Login to MediaSense GUI using an administrator user created during installation.
2. Proceed to the Cisco MediaSense Administration page.
3. Select Administration -> Unified CM configuration
4. Select the CUCM server from the Available AXL Service Providers list.

5. Enter the API user created on the CUCM for communicating with MediaSense.
6. Select the CUCM server from the Available Call Control Service Providers list.
7. Click Save

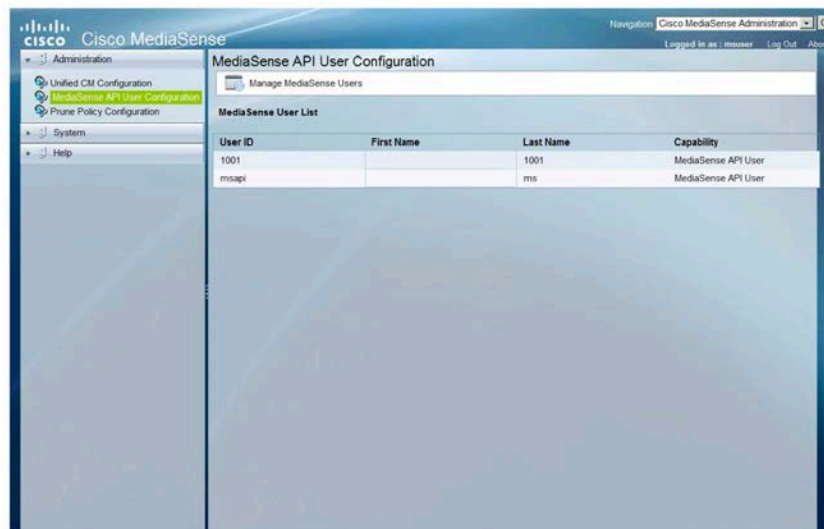


### 19.1.2 MediaSense API User Configuration

Configure a MediaSense API user to playback audio recording from the server. This user will also be configured on the REM to enable GUI based playback options.

Steps:

1. Login to MediaSense server as an administrator user.
2. Proceed to Administration -> MediaSense API User Configuration
3. Click on Add New
4. Enter details for a user with permissions to invoke playback.
5. Click Save.



### 19.1.3 Prune Policy Configuration

Based on need you can configure how long the audio records should remain on the MediaSense server disks. By default it will delete files after 60 days of archiving.

## Steps:

1. Login to MediaSense server as an administrator user.
2. Proceed to Administration -> Prune Policy Configuration
3. Enable or disable 'Automatically prune recordings after they are more than "" days' as per need.
4. Save or Reset as required.
5. Restart MediaSense service once the change is complete.

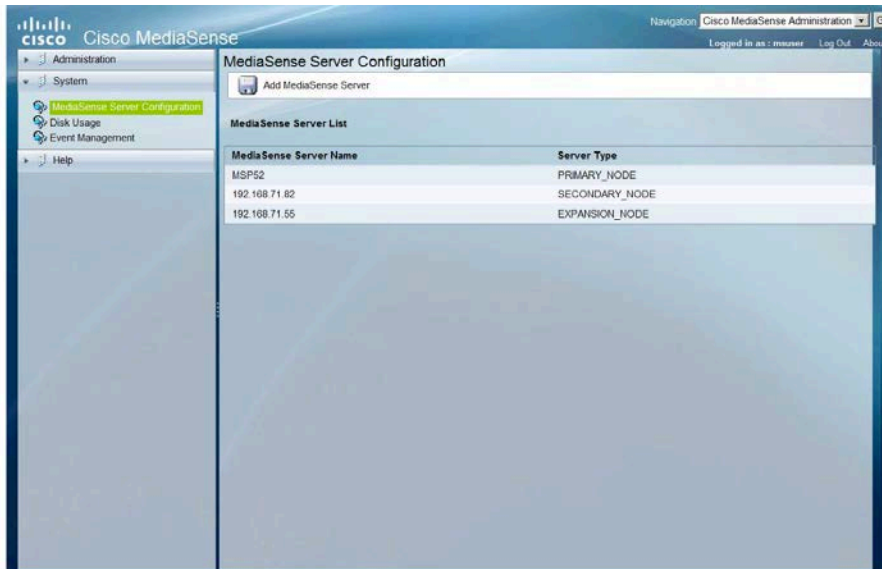


### 19.1.4 MediaSense Server Configuration

Here we add the MediaSense Server(s) into the system. In case we have more than one server, the same needs to be listed in the CUBE configuration for forking. MediaSense uses its own algorithm to select the most favored servers and hence establishes a form of load balancing.

## Steps:

1. Login to MediaSense server as an administrator user.
2. Proceed to System -> MediaSense Server Configuration
3. Click on Add MediaSense Server.
4. Provide the IP address and desired information.
5. Click on Save.
6. Restart MediaSense service once the change is complete.



## 19.2 Cisco Unified Border Element (CUBE)

Cisco Unified Border Element or CUBE is a B2BUA (Back-to-back User Agent), which means that CUBE negotiates two call-legs, each of which is independently negotiated between the RE endpoints and CUBE. Therefore, CUBE sinks and re-originates the media towards the other endpoint. CUBE does do a cursory examination of the RTP payload while it sinks and sources the stream and this means that the CUBE support of the codecs or the functionalities is necessary to enable the same between the two endpoints

CUBE is configured as a media forking point by using “dial-peer” configurations. For these configurations, the endpoints must have a Directory Number (DN) number since dial-peers are based on these numbers.

When the CUBE encounters a call that needs to be recorder, it generates one SIP invite towards MediaSense with two “m” lines, one for each audio track stored separately.

### 19.2.1 CUBE/Forking Configuration

We will do a deep dive into the configuration with highlighting the specific configurations for this Remote Expert setup with **text**:

```
voice translation-rule 1

rule 1 /^3+/ //

!

!

voice translation-profile discard3
```

```
translate called 1

!

!

!

!--- create MediaSense class for forking

media class 3

recorder parameter

media-recording 3000 3001 3002

!

!

interface Embedded-Service-Engine0/0

no ip address

shutdown

!

.

.

.

.

.

!

ip http server

!

!

mgcp behavior rsip-range tgcp-only

mgcp behavior comedia-role none
```



```
mgcp behavior comedia-check-media-src disable
mgcp behavior comedia-sdp-force disable
!
mgcp profile default
!
!
!---- Apply MediaSense media class to the incoming dial-peer
dial-peer voice 1000 voip
description inbound and forking
rtp payload-type cisco-codec-fax-ack 110
rtp payload-type cisco-codec-video-h264 97
session protocol sipv2
incoming called-number 2...
voice-class codec 1 offer-all
voice-class sip asserted-id pai
media-class 3
!
!---- Send the call to CUCM to handle routing to the expert endpoint
dial-peer voice 2000 voip
description outbound
destination-pattern 2...
rtp payload-type cisco-codec-fax-ack 110
rtp payload-type cisco-codec-video-h264 97
session protocol sipv2
session target ipv4:192.168.71.40:5060
voice-class codec 1 offer-all
```

```
!  
!---- Send call to MediaSense expansion  
dial-peer voice 3000 voip  
description MediaSense-expansion  
destination-pattern 3333  
session protocol sipv2  
session target ipv4:192.168.71.55  
session transport tcp  
voice-class sip options-keepalive  
!  
!---- Send call to MediaSense primary  
dial-peer voice 3001 voip  
description MediaSense-primary  
destination-pattern 3333  
session protocol sipv2  
session target ipv4:192.168.71.52  
session transport tcp  
voice-class sip options-keepalive  
!  
!---- Send call to MediaSense secondary  
dial-peer voice 3002 voip  
description Mediasense-secondary  
destination-pattern 3333  
session protocol sipv2  
session target ipv4:192.168.71.82  
session transport tcp
```

```
voice-class sip options-keepalive
```

```
!
```

```
!
```

```
!
```

```
gatekeeper
```

```
shutdown
```

```
!
```

```
!
```

## 19.3 Conferencing/Transfers

In the Remote Expert Solution, for conferencing call flows we use a Codian MCU 4610 registered to CUCM as the Video Conference Bridge.

### 19.3.1 MCU 4610 Configuration

Below, you will find quick steps to configure the Media Conferencing Unit for setting up the Video Conferencing feature in the Remote Expert Solution.

Steps:

1. Login to the MCU as Administrator user
2. Ensure licenses are uploaded and the build version on the MCU is as required.
3. Proceed to Home-> Network -> PortA/B and configure the basic networking/reachability.
4. Ensure under Home -> Network -> Services, SIP is enabled and the port is 5060.
5. Check the settings under Home -> Settings -> Conferences has the desired configurations.
6. Under Home -> Settings -> SIP, make sure that SIP registrar type is Standard SIP
7. Select HD for the Home -> Settings -> Media Port's Media Port Mode.
8. Save configuration and exit.

Once this is complete, we need to add this MCU as a Cisco TelePresence MCU in the CUCM Conference Bridge add page. Point the IP address in this configuration to the IP address of the MCU. Also provide HTTP credentials for the Conference Bridge configuration.

## 20 Specialized Customer Pod peripheral integration

---

The Remote Expert Smart Solution supports extensions allowing specialized peripherals to be installed at the Media Conferencing Unit for setting up Customer Pods and integrated with the Video Conferencing feature in the solution, including:

- Keypads
- Magnetic Card Readers

For more information on specialized peripheral integration with the Remote Expert Solution Smart solution, please refer to Chapters X-Y of the *Deploying REM for the Remote Expert Smart Solution 1.8 Guide*.

Steps:

1. Login to the MCU as Administrator user
2. Ensure licenses are uploaded and the build version on the MCU is as required.
3. Proceed to Home-> Network -> Port A/B and configure the basic networking/reachability.
4. Ensure under Home -> Network -> Services, SIP is enabled and the port is 5060.
5. Check the settings under Home -> Settings -> Conferences has the desired configurations.
6. Under Home -> Settings -> SIP, make sure that SIP registrar type is Standard SIP
7. Select HD for the Home -> Settings -> Media Port's Media Port Mode.
8. Save configuration and exit.

Once this is complete, we need to add this MCU as a Cisco Telepresence MCU in the CUCM Conference Bridge add page. Point the IP address in this configuration to the IP address of the MCU. Also provide HTTP credentials for the Conference Bridge configuration.

## 21 Custom Branding the Remote Expert Smart Solution

---

The default branding assets installed in Section 15.2 are sufficient for verifying basic system operation. Custom branding assets will need to be designed, developed, tested in conjunction with the solution and approved by the enterprise customer before the solution can be placed into actual trials or production.

Please refer to Chapters 2 and 3 of the [Cisco Remote Expert Manager 1.8 Administration Guide](#) for information on aspects of customizing the graphical user interface of the Remote Expert Smart Solution and how to deploy these customizations.

## 22 References

---

Please refer to following supporting documents for more detailed information.

1. Cisco Remote Expert Manager Home Page:  
[http://www.cisco.com/en/US/products/ps12838/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps12838/tsd_products_support_series_home.html)
2. Cisco Remote Expert Manager 1.8 Installation Guide:  
[http://www.cisco.com/en/US/docs/solutions/Enterprise/collaboration/Remote\\_Expert/REM\\_1.8/re\\_ig.pdf](http://www.cisco.com/en/US/docs/solutions/Enterprise/collaboration/Remote_Expert/REM_1.8/re_ig.pdf)
3. Cisco Remote Expert Manager 1.8 Administration Guide:  
[http://www.cisco.com/en/US/docs/solutions/Enterprise/collaboration/Remote\\_Expert/REM\\_1.8/re\\_ag.pdf](http://www.cisco.com/en/US/docs/solutions/Enterprise/collaboration/Remote_Expert/REM_1.8/re_ag.pdf)
4. Cisco Remote Expert Manager 1.8 Agent Desktop User Guide:  
[http://www.cisco.com/en/US/docs/solutions/Enterprise/collaboration/Remote\\_Expert/REM\\_1.8/re\\_ug.pdf](http://www.cisco.com/en/US/docs/solutions/Enterprise/collaboration/Remote_Expert/REM_1.8/re_ug.pdf)
5. Cisco Remote Expert Manager 1.8 Troubleshooting Guide:  
[http://www.cisco.com/en/US/docs/solutions/Enterprise/collaboration/Remote\\_Expert/REM\\_1.8/re\\_tg.pdf](http://www.cisco.com/en/US/docs/solutions/Enterprise/collaboration/Remote_Expert/REM_1.8/re_tg.pdf)
6. Cisco Remote Expert Manager 1.8 Release Notes:  
[http://www.cisco.com/en/US/docs/solutions/Enterprise/collaboration/Remote\\_Expert/REM\\_1.8/re\\_rn.pdf](http://www.cisco.com/en/US/docs/solutions/Enterprise/collaboration/Remote_Expert/REM_1.8/re_rn.pdf)



Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

Asia Pacific Headquarters  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Europe Headquarters  
Cisco Systems International BV  
Amsterdam, The Netherlands

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](http://www.cisco.com/go/offices).

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website 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. (1002R)