



Quick Installation and Configuration Steps for Virtual Expert Management

Introduction

This section is based on internal guides created by Laurent Pham and Shahazd Ali. It has been expanded to include all VEM components, and updated to reflect the specific settings and items used in the validation lab. Figure B-1 depicts the components and endpoints that are covered.



Figure B-1 Virtual Expert Management Protocols and Services

Prerequisites

Cisco recommends that you should have knowledge of the following topics:

- Cisco Unified Communication Manager (CUCM)
- Cisco Unified Intelligent Contact Management (CUICM)
- Cisco Unified Cisco Voice Portal (CUCVP)
- Cisco Voice Gateways and VXML Gateways
- Cisco Unified Expert Advisor
- Cisco Unified Presence and SIP Proxies
- Cisco Unified TelePresence
- Cisco Unified Video Advantage
- Cisco Unified MeetingPlace
- Cisco WebEx Meeting
- Cisco WebACD
- Cisco WebEx Access Anywhere

Preparing the Environment

System Information

- This guide assumes that CUCM is installed and configured with appropriate endpoints. For a quick guide to install and configure CUCM with CVP and VXML GW, refer to the following URL: https://supportforums.cisco.com/docs/DOC-1374
- All domain controllers in your domain or forest must be running Windows Server 2003 with the domain functional level set to Windows Server 2003, thereby all domain- and forest-wide features needed are available.
- Before installing ICM software components, the computers must have the Microsoft Windows operating system—including SNMP and (for Windows 2003) WMI and, for some components, Microsoft SQL Server database management software installed. See Figure B-2.

Figure B-2 System Installer

Sub <u>c</u> ompone	ents of Management and Monitoring Tools:		
🗌 🎒 Conr	ection Manager Administration Kit	1.1 MB 📐	
🗌 🖸 Conr	ection Point Services	0.2 MB	
🗹 🚚 Netw	ork Monitor Tools	2.3 MB	
🛛 🗹 📇 Simp	le Network Management Protocol	0.9 MB	
🗹 📙 WMI	SNMP Provider	1.1 MB	
🗹 📇 WMI	Windows Installer Provider	0.6 MB	
Description:	Allows client applications to access Windows In Windows Management Instrumentation (WMI).	nstaller information through	228073

• This installation includes setting up the Windows Active Directory services for ICM software. Setting up Active Directory entails adding the Cisco Root Organizational Unit, one Facility Organizational Unit, and one Instance Organizational Unit to the Active Directory Schema. These steps require domain admin-level access.

For more information, refer to the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* and the *SNMP Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* at the following URLs:

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_g uides_list.html

CCE components that operate on Cisco IPT Windows OS 2003 Enterprise Edition must also have the following services installed and started:

- DNS Service—Required for AD
- Replication Service—Required for AD
- Task Scheduler Service—Required for ICM Installation
- Install WMI Windows Installer Provider—Required for ICM Router Installation
- NT LM Security Support Provider—Required for AD
- File Replication—Required for AD

The CUICM components Router, Logger, AW, PG, and CTIOS Server must communicate with the Active Directory server and join a domain. In this validation setup, the Active Directory Domain Controller and DNS Server are already set up and have been used in previous solutions. For more information on installing and setting up Active Directory, refer to the Windows 2003 server administration guides.

SQL server is a required component for the Logger platform. Installation of this software is covered in the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* referenced above.

ICM software requires Microsoft SQL Server databases on each Logger, Historical Data Server (HDS), and each Real-time Distributor Admin Workstation (SQL Server is not required for Client AWs). SQL Server must be installed on each of these computers before you install the ICM software.

Virtualization Support

Beginning with Cisco Unified ICM and Unified Contact Center Enterprise and Hosted Editions Release 7.5(3), servers can be consolidated by deploying a virtualization solution for Client Administrative Workstations (AWs) and certain Peripheral Gateways (PGs) on the VMware platform. For the virtualization requirements, mapping to discrete servers, and CPU processor and RAM requirements for each of the supported PG and Client AW virtual machines (VMs), refer to the latest version of the *Hardware & System Software Specification (Bill of Materials) for Cisco ICM/IPCC Enterprise & Hosted Editions*, available at the following URL:

http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_implementation_design_guides_1 ist.html

Before you incorporate virtual machines into your contact center design and deployment, you must read through and follow the guidelines and restrictions described in the *Virtualization Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*, available at the following URL:

http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_user_guide_list.html

Other Unified ICM and Unified CCE components, such as the CallRouter, Logger, AW Distributor, HDS, WebView Server, and CAD Server, as well as the Cisco Unified Contact Center Management Portal (Unified CCMP), and Cisco Unified Intelligence Suite, are not supported in a virtualized environment at this time.

Hardware Components

The following are the hardware components of the IPCC laboratory system:

- Two Cisco 794x/796x/797x series IP phones as Expert Advisor user phones
- One MCS Server for CUCM
- Two servers running Windows 2003 Enterprise Edition for CUICM Enterprise Components in duplex mode:
 - Router
 - Logger
 - AW
 - CUCM PG
 - CVP VRU PG
 - CTIOS Gateway or CTIO PG
 - CTIO Server
- Windows 2003 Enterprise Edition-based server running the following CVP components:
 - CVP Call Server
 - CVP Media Server
 - Microsoft IIS Web Server
- One MCS server for Cisco Unified Presence
- One MCS server for Cisco Unified Expert Advisor
- Windows XP based agent PC
- Cisco 3845 Router
 - Ingress PSTN Gateway
 - VXML Gateway
- PSTN Simulator (CUCME gateway with cross over T1 PRI cable connected to CVP Gateway could be used)

Unified CCE 7.5(1) components are supported only on Cisco MCS or MCS-equivalent servers. For further specifics on hardware requirements including recommended platform sizing guidelines (not specific brands or models of servers), based on the types of available hardware systems, refer to the *Hardware and System Software Specification (Bill of Materials) for Cisco Unified ICM/Unified Contact Center Enterprise & Hosted, Release 7.5(1)* at the following URL:

http://www.cisco.com/en/US/products/sw/custcosw/ps1844/products_user_guide_list.html

Appendix B Quick Installation and Configuration Steps for Virtual Expert Management

Software Components

The software release is based on the system Release 7.1(3):

- Cisco IOS Software Releases 12.4(24)T1 Voice Feature Set on the VXML Gateway
- Cisco Unified Communication Manager version 7.1(3)
- Cisco Unified Presence Server 7.0(5)
- Cisco Unified ICM version 7.5(6)
- Cisco Unified CVP version 7.0(2)
- Cisco Unified Expert Advisor 7.6(1) SR1
- Cisco CTI Object Server 7.5(6)
- JTAPI Client version is CUCM bundled

Installation

The following component need to be installed:

- Install CUCM (Publisher and Subscriber)
- Install TelePresence endpoints
- Install CCE / ICM
- Install CVP
- Install CUP and CUPC Clients
- Install EA

Pre-requisite:

• Be familiar with CUCM, Unified CCE, and Unified CVP



This appendix does not cover the basic installation of Unified CCE and Unified CVP. It assumes you have basic knowledge of CUCM, Unified CCE, and Unified CVP.

CUCM Installation

- In VMWare environment, a minimum of 72 GB disk is required
- Version: 7.1.3.10000-11
- Make sure the CTI Manager and Cisco AXL Web services are running

CCE Installation

To install 7.5(6), 1 UCCE 7.5(1), many need to be installed first and then upgraded to 7.5(6) (the upgrade is available on cisco.com).

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*. For details, refer to the following URLs:

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns818/landing_contact_ctr.html

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_technical_reference_list.html

The ICM Setup program allows you to install, update, and configure your ICM software. It is located on your ICM CD. Run Setup on each machine in the ICM system: each CallRouter, each Logger, each Peripheral Gateway (PG), and each Admin Workstation. At 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.

Installation of each of the ICM components is performed through the ICMSetup application. This application is located in the **ICM\bin** directory of the DVD as well as the ICM directory after an installation has already been accomplished.

After executing the ICMSetup program, the **ICM Component Selection dialog** box appears where the buttons used to install the components are displayed. The following components were used in the validation testing:

- Admin Workstation
- Router
- Logger
- Peripheral Gateway
- CTI Server
- CTI OS Server

About the 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 CallRouter, 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.



During the installation of the Central Controller and Administration and WebView 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.

About ICM Component Installation Order

You can install the various components in the order in which they are treated in this appendix. In general, there is a great deal of flexibility in the order of installation, provided that you know the names and locations for the various components beforehand. However, the following presents the standard approach:

- Step 1 Install either the CallRouter or the Logger first. It does not matter in which order you install the CallRouter and Logger.
- Step 2 Install both the CallRouter and the Logger before you install an Admin Workstation (AW).
- Step 3 ICM Setup and Installation Guide Cisco Unified ICM/Contact Center Enterprise & Hosted 7.5(1)
- Step 4 If you are using WebView, install it after you have installed the Real-time Distributor AW.
- Step 5 Install the CallRouter, Logger, and AW before you install the Network Interface Controller (NIC) and Peripheral Gateway (PG), but it does not matter in which order you install the NIC and PG.
- Step 6 Install the CTI Server after you have installed the CallRouter, Logger, AW, NIC, and PG.

Creating an ICM Instance

- Before any ICM components can be installed and 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

Configure Domain Manager

Step 1 Start the Cisco Unified ICM installation by running the ICMSetup.exe application on the CD or local directory as appropriate.

Click the Domain Manager. See Figure B-3. Step 2

Figure B-3	Domain Manager	
Cisco ICM Setup		×
- ICM Instances -	Add Edit Edit Delete	
Upgrade All	Domain Manager urity Hardening Help Exit Setup	28074

Select the desired domain from the list on the left and click ADD, then click OK. See Figure B-4. Step 3

Select Domains		×
Enter domain name:	:	Selected domains:
Filter domain choices © Forest © Trusted © Both (Forest and Trusted)		
Choose domains: CISCO-IRN.COM	A <u>d</u> d >	
	Add All >>	
	OK	CancelHelp

Figure B-4 Selecting Domain

- **Step 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**.
- **Step 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**.
- **Step 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**. See Figure B-5.

ICM Domain Manager File Help	X
CISCO-IRN.COM	Domains Select Select Add Remove Add Remove Add Remove Instance Add Remove Security group Members
	Help Close

Figure B-5 Adding Instance Name

Step 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.

At least one ICM instance must be added before you can install any ICM components.

\$. Note

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. Refer to the *Staging Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted*.

- **Step 8** 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.



The ICM Instance Name is the name of the Instance Organizational Unit.

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



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

Step 1	Click OK	. See	Figure	B-6 .
--------	----------	-------	--------	--------------

Figure B-6	Creating an in	stance	
Cisco ICM Setup		X	
- ICM Instances	Add	ance Components	
	Add Instance		×
	Instance Information-		
	Domain	cisco-irn.com	
Upgrade All	Facility	cisco_icm_facility	
	Instance Name	icm 💌	
	Instance Number	0	
Prompt for Secur	The selected facility select another facility instance OU to this fa	does not contain an available ICM instance OU. Please , or use the ICM Domain Manager to add a new acility.	
		Domain Manager	
	0	K Cancel Help	228077

Step 2 You can now add ICM Instance components. First create and install Router and Logger ICM Servers.When installed together they are commonly referred to as a Rogger Server.

Refer to Chapters 5 and 6 of the ICM Setup and Installation Guide at the following URL:

http://www.cisco.com/en/US/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_7_5/installation/guide/icm75instl.pdf

Install the Router and Logger

Call Router Installation

The CallRouter (generally referred to in this document simply as the *Router*) is the component that contains the contact routing logic and makes all routing decisions. It receives contact routing requests and determines the best destination for each contact. It also collects information about the entire system. This appendix explains how to install the CallRouter software and perform some basic configuration. For this configuration, you must know the visible and private network addresses (either host names or IP addresses) of the CallRouter and, for a duplexed configuration, the addresses of the CallRouter on the other side. The CallRouter and Logger are typically on separate computers. However, in small contact center configurations they can both be on the same computer. See Figure B-7.



Step 1 In the ICM Setup application, click the **Add** button on the right under **Instance Components**. See Figure B-8.

Figure B-8



A new dialogue window will appear where you will be able to select the Router component. See Figure B-9.

Router Properties		×
	Node Manager properties Production mode Auto start at system startup Duplexed Router Database routing Application gateway Remote Network Routing NAM ID: No system reboot on error Side Side A Side B	
	Help < <u>B</u> ack <u>N</u> ext > Cancel	

Step 2 For high availability installations select the Duplexed Router option and click Next.

Do not select any Network Interface Controllers. Leave all the options as default. The Customer ID is insignificant for this solution. See Figure B-10.

Network interface	e controllers		
	Configure	MCI:	Configure
AUCS INAP:	Configure	Nortel:	Configure
CAIN:	Configure	T NTL:	Configure
CRSP:	Configure	🔲 Sprint:	Configure
🗖 CWC:	Configure	SS7IN:	Configure
🗖 СКТМР:	Configure	🔲 Stentor:	Configure
INCRP:	Configure	TIM INAP:	Configure
C ICRP:	Configure		
Customer ID:	0	MDS timed delivery qu Interval: 50 Threshold: 50	ueue
	H	lelp < Ba	ack <u>N</u> ext > Cancel

Figure B-10

Step 3 Click Next.

For the lab validation, two peripheral gateways were used; one for CUCM and another as VRU PG for CVP and expert advisor.

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". See Figure B-11.

Figure B-11

I	Peripheral Gateway devices			1
	Peripheral Gateway Devices (1-80) :	1-3		
			Advanced	8082
				8

Step 4 Accept the current settings and click on **Next** for the following screens.

It is best practice to use IP addresses rather the hostnames when identifying the public and private interfaces for the Router. The following image and other similar installation screens during CUICM component installation will be similar. See Figure B-12.

	Network Interface Properties	Router private interfaces Node A: Node A high: Node B high: Router visible interfaces Node A: Node A high: Node B: Node B high:	192.168.9.17 192.168.9.17 192.168.9.18 192.168.9.18 192.168.45.141 192.168.45.141 192.168.45.142 192.168.45.142	QoS	X
Help < <u>B</u> ack <u>N</u> ext > Cancel		Help < Bac	k <u>N</u> ext≻	Cancel	00000

Figure B-12

Note

If the CallRouter is simplexed, enter **localhost** in both the **B** and **B high** fields.

Step 5 After entering the Router interface IP addresses click Next. See Figure B-13.

Check Setup Information		
Setup has enough information to begin the co If you want to review or change and of the se If satisfied, click Next to begin configuring the	nfiguration operation. ttings, click Back. Router.	
Current Settings:		
Setup Type: Router, side A Target Directory: C:\icm Configuration: Router is duplexed Microsoft Windows DHCP Media Sense is dis	sabled.	
tallShield		
	< <u>B</u> ack <u>N</u> ext >	Cancel

Step 6 At the ICM setup, review the installation settings and click *Next* to complete the installation of the Call Router.

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. See Figure B-14 and Figure B-15.







Step 7 Select production, Auto startup and Duplexed logger options, then click Next. See Figure B-16.

Figure B-16

Logger Component Propertie	5	×
	Customer support Phone home Configure	J
	Outbound Option Enabled Configure	J
A	Logger database configuration Purge	
CO		
	Help < <u>B</u> ack <u>N</u> ext > Cancel	

Step 8 Click Next. See Figure B-17.

Fiar	iro	R.	17
гии	ne.	D-	17

Network Interface Properties	- Router private interfaces	192.168.9.17 192.168.9.18 192.168.9.17 192.168.9.17 192.168.9.18	×
Help	< <u>B</u> ack <u>N</u> e:	kt > Cancel]

- Step 9 Configure the public and private Router and Logger interfaces using the IP address. Click Next.
- **Step 10** At the end of the ICM setup, review the installation settings and click **Next** to complete the installation of the Call Logger.

Create ICMDB on Logger

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.

For more information on using the ICMDBA tool, refer to the ICM Administration Guide for Cisco Unified ICM/Contact Center Enterprise &Hosted.

Once the proper size is determined, run the **icmdba.exe** file from the local ICM directory to create and configure the new database. See Figure B-18.

Figure B-18

alala ICM-A - ICMDBA	
<u>File D</u> atabase <u>V</u> iew <u>S</u> erver	D <u>a</u> ta <u>H</u> elp
9	
Gervers Gervers Gervers Gervers Gervers Gervers Gervers Gervers Gervers Gervers	
Tempdb	Create
	Delete Estimate Expand Recreate
	Properties
For Help, press F1	-

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. See Figure B-19.

Create Database			X
Instance: icm1			Create
Configuration			Cancel
DB Type sideA		Region North America	Help
ICM Type Standard		Partitions	
Storage			
Device Name	Type Drive	Size	
Contemporation Contem	data C	1400.00MB	
icm1_sideALogC	log C	100.00MB	
			8

Figure B-19

You will notice a screen similar to screen shown in Figure B-20 and once the database is created successfully click **OK**.



Installing the Admin Workstation

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) is the human interface to the ICM software. It 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. See Figure B-21.





Step 1 From the ICM Setup applications, select **Add** for the ICM instance and then "**Admin Workstation**". See Figure B-22.

Admin Workstation Properties	5	×
	Admin Workstation Configuration Client (No Real-time Distributor) Real-time Distributor AW Type Standard Limited AW Network AW (NAM) Network AW (CICM) Production Mode Target drive:	
	Help < <u>B</u> ack <u>N</u> ext > Can	cel

Step 2 Select Next. See Figure B-23.

Figure B-23

Real-time Distributor Node Pro	perties	×
	Node Manager Properties Auto start at system startup Agent Re-skilling Web Tool CMS node	
	 Internet Script Editor Server Service Account Management Do not modify service accounts Setup creates service accounts User manages service accounts 	
	Help < <u>B</u> ack <u>N</u> ext > Cancel	228094

Step 3 Select Next. See Figure B-24.

Figure	B-24
riguie	D-24

Real-time Distributor Properties				
	Admin site name:	icm-admin		
	Second distributor for site Central controller preferred sid Central controller side A Central controller side B Database WebView Database Historical Data Server Partitioning WebView Server Remote WebView Server Central Controller Bouter side A:	Is SQL Server Drive: C Apply SQL Security Hardening (s) Configure		
	Router side B:	192.168.45.142		
	Logger side A:	192.168.45.141		
	Logger side B:	192.168.45.142		
	Help < <u>B</u> ack	Cancel 8		

Step 4 Select Next.See Figure B-25.

Figure	B-25
--------	------

Admin Workstation Client Prope	ties	×
	Real Time Distributors Primary distributor: Secondary distributor: Workforce Management Outbound Option Support	icm-admin
	Help < <u>B</u> ack <u>N</u>	ext > Cancel 00

Step 5 Verify Setup parameters and select **Next** to finish. See Figure B-26.

Figure B-26

ICM Setup: icm-AW		×
Check Setup Information		
Setup has enough information to begin the co If you want to review or change and of the set If satisfied, click Next to begin configuring the	nfiguration operation. ttings, click Back. Admin Workstation.	
Current Settings:		
Setup Type: Admin Workstation Distributor Target Directory: C:Vicm Configuration: Admin is a Realtime Distributor Backup distributor: Router: 192.168.45.141/192.168.45.142		×
InstallShield		
	< <u>B</u> ack <u>N</u> ext>	Cancel

Step 6 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. See Figure B-27.

Figure B-27

🛂 Initialize Local Database		
Table name	Elapsed time (sec)	Rows copied
ICR_Instance		
ICR_Node		
Customer_Definition		
Customer_Options		
Logical_Interface_Controller		
Physical_Interface_Controller		
Agent_Desk_Settings		
Peripheral		
Cfg_Mngr_User_Desktop_Snap		
Cfg_Mngr_App_Snapshot_State		
Cfg_Mngr_User_Menu		
Cfg_Mngr_View		▼
		•
Connections		Start
Instance name: icm1		<u></u>
Local Viem1 awdb		<u>C</u> lose
Cautal 102.100.02.120View1 vide	*	8
Lentral 192.168.93.130\lCm1_side	A	

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.

AW Configuration Manager CUCM PG Setting

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

Note

Although a PG can consist of a pair of duplexed computers, only one of them is active at a time, so that ICM software sees it as a single logical and physical PG.

Primary CTI OS Server

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.

Create a new Agent Desk Settings list as follows:

- **Step 1** Open the Configurations Manager on the AW.
- Step 2 Select the Agent Desk Settings List option under the Tools >Explorer Tools group.
- Step 3 Click Retrieve.
- Step 4 Click Add.
- **Step 5** Enter an appropriate list name such as **Agent_Desk_Settings_1**.
- **Step 6** Enter a proper description.
- **Step 7** Set the Ring no Answer time to **10**.
- **Step 8** Set the Wrap up time to **20**.
- Step 9 Click Save. See Figure B-28.

Figure B-28

Agent Desk Settings List	-	
_Select filter data	Attributes	
	Name * Agent_Desk_Settings_1	
Optional Filter Condition Value	Ring no answer time 10 seconds (1 · 120)	
None	Ring no answer dialed number None>	
Save <u>R</u> etrieve Cancel filter changes	Logout non-activity time seconds (10 - 7200)	
Agent Desk Settings	Work mode on incoming * Optional	
Agent_Desk_Settings_1	Work mode on outgoing * Optional	
	Wrap up time 20 seconds (1 - 7200)	
	Assist call method Consult	
	Emergency alert method Consult	
	Description CUCM Agent Desk Global Setting #1	
	Miscellaneous	
	☐ Idle reason required	
	Logout reason required Ive Local private network	
	Auto record on emergency C Operator assisted PBX	
	Enable Cisco Unified Mobile Agent	
	Mobile agent mode Agent chooses	
Add Delete Revert	Save Close Heir	p
IM Instance: icm		

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

Create a new Agent Desk Settings list as follows:

- **Step 1** Open the Configurations Manager on the AW.
- **Step 2** Select the **Media Routing Domain List** option under the **Tools > Explorer Tools** group.
- Step 3 Click Retrieve.
- Step 4 Click Add.
- **Step 5** Enter an appropriate list name such as **Cisco_Voice**.
- **Step 6** Enter a proper description.
- Step 7 Set the Media Class to Cisco_Voice.
- Step 8 Click Save. See Figure B-29.

Attributes					
Name	* Cisco_Voice				_
Media routing domain ID	* 1				
Media class	* Cisco_Voice				
– Task –			Ove Media Def	rride a Class ault	
Life	0	seconds	Ŀ	7	
Start timeout	0	seconds	Г	7	
Max duration	0	seconds	Г	7	
Calls in Queue			_		
Max					
Max per call type					
Max time in queue		seconds			
Service level threshold	* 30				_
Service level type	* Ignore Abandoned Calls				
Interruptible					
Description	Default Media Routing D	omain for Ci	sco_V	pice	
		<u>S</u> av	e	<u>C</u> lose	

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

There are several methods for creating PGs and their underlying Peripheral Interface Managers (PIMS). For this solution, two PGs are created. One PG is generic and have the CUCM and VRU_CVP PIMS, the other PG is for Expert Advisor and have the EA PIM. Each ICM server set that is deployed can have a maximum of two Peripheral Gateways. 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.

Create the first peripheral gateway logical controller as follows:

- **Step 1** Open the Configurations Manager on the AW.
- **Step 2** Select the **PG Explorer** option under the **Tools > Explorer Tools** group.
- Step 3 Click Retrieve.
- Step 4 Click Add PG.
- **Step 5** Enter an appropriate name such as **Generic_PG_1**.
- **Step 6** Enter a proper description.

- **Step 7** Set the client type to **PG Generic**.
- **Step 8** Set the IP address for the primary and secondary CTI Servers.
- Step 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. See Figure B-30.

Figure B-30

Logical Controller		
Logical controller ID:+ 5000	Physical controller ID: ★ 5000	l
Name:	* Generic_PG_1	l
Client type:	PG Generic 💌	L
Configuration parameters:		L
Description:	CTI Server to have CTI agents	L
Physical controller description:		L
Primary CTI address:	192.168.45.151	L
Secondary CTI address:	192.168.45.152	1410
		Į ŝ

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

Step 1 Select the Generic_PG_1 PG that was just added from the PG explorer results on the left.

Step 2 Click Add Peripheral.

- **Step 3** Enter an appropriate peripheral name such as **CCM_PIM_1**.
- **Step 4** Select the Client Type as **CallManager/SoftACD**.
- **Step 5** Select the Default Desk Settings option that was created earlier **Agent_Desk_Settings_1**.
- **Step 6** Enter a proper description.
- Step 7 Check the Enable post routing option.
- Step 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 ICMSetup. See Figure B-31.

Skill Group Mask 🗍 B	outina el	lient	Defau	lt route	Perir	oberal Monitor	
Peripheral	Ac	dvanced	Derdu		Agent Di	stribution	
Peripheral ID:	* 5000)			-		
Name:	* CCN	1_PIM_1	1				
Peripheral name:	* CCN	1_PIM_1					
Client type	* Call	Manage	r/SoftA0	D		•	
Location:							
Abandoned call wait time:	* 5						
Configuration parameters:							
Call control variable map:							
Default desk settings:	Age	nt_Desk	_Settin;	gs_1		-	
Peripheral service level typ	e:* Calo	culated b	y Call C	enter		~	1
Description:	VEN	1 based	ССМ				
Enable post routing:	~	Per	ipheral a	auto conf	igured:	Г	
		<u>S</u> a	ive		lose	<u>H</u> elp	1000

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

- **Step 1** Enter an appropriate name and Peripheral name such as **CUCM_RC**.
- Step 2 Select the Client Type as PCC/Enterprise Agent.
- **Step 3** Select the Default media routing domain option to **Cisco_Voice**.
- **Step 4** Enter a proper description.
- Step 5 Click Save. See Figure B-32.

Figure B-32

Peripheral	Í	Advanced			gent Distributi	on	
Skill Group Mask	Routing	; client	Defaul	t route	Peripheral	Monito	r
Name:	*	CUCM_F	Rd		D: * 5000		
Timeout threshold:	*	1500					
Late threshold:	*	500					
Timeout limit:	*	10					
Default media routing do	omain:	Cisco_V	oice			•	
Default call type:		NONE				•	
Configuration parameter	s:						
Dialed Number/Label m	ap: *	Do not u	ise DN/La	abel map		•	
Client type:	*	IPCC / E	Enterprise	Agent		•	
Description:		CUCM re	outing to c	lient			
Network routing client:							
Network transfer preferm	ed:						
							i i i i

Step 1 On the Default Route tab ensure that Cisco_Voice is selected. See Figure B-33.

Figure B-33

Skill Group Mask Routing client Default route Peripheral Monitor						
Current default route en	ries					
Media routing domain	Route					
Cisco Voice						
- N - 1						
New			Delete			
Media routing domain: 3	Cisco_Voice		•			
Route:	NONE					

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

- Step 1 Select the Generic_PG_1 PG that was added from the PG explorer results on the left.
- Step 2 Click Add Peripheral.
- **Step 3** Enter an appropriate name and peripheral name such as CVP_VRU_PIM_2.
- **Step 4** Select the Client Type as **VRU**.
- **Step 5** Select the Default Desk Settings option to **NONE**.
- **Step 6** Enter a proper description.
- Step 7 Check the Enable post routing option.
- Step 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. See Figure B-34.

Skill Group Mask Rol Peripheral	uting client Default Advanced	route Peripheral Monitor Agent Distribution
Peripheral ID:	* 5001	
Name:	CVP_VRU_PIM_2	
Peripheral name:	CVP_VRU_PIM_2	
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 Ce	nter 🔽
Description:	VRU for CVP Call rou	ting
Enable post routing:	Peripheral au	uto configured: 🗖

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

- Step 1 Enter an appropriate name and Peripheral name such as CVP_VRU_PIM.
- **Step 2** Select the Client Type as **VRU**.
- **Step 3** Select the Default media routing domain option to **Cisco_Voice**.
- **Step 4** Enter a proper description.
- Step 5 Click Save. See Figure B-35.

Figure B-35

Peripheral	Advanced	Agent Distribution
Skill Group Mask Roul	ting client Defau	It route Peripheral Monitor
Name:	* CVP_VRU_PIM	ID:* 5001
Timeout threshold:	* 2000	
Late threshold:	* 1000	
Timeout limit:	* 10	
Default media routing domain:	Cisco_Voice	•
Default call type:	NONE	▼
Configuration parameters:		
Dialed Number/Label map:	* Do not use DN/L	.abel map 💌
Client type:	* VRU	•
Description:		
Network routing client:		
Network transfer preferred:		

Create the second peripheral gateway logical controller for the Expert Advisor as follows:

Step 1 Open the Configurations Manager on the AW.

- **Step 2** Select the **PG Explorer** option under the **Tools > Explorer Tools** group.
- Step 3 Click Retrieve.
- Step 4 Click Add PG.
- **Step 5** Enter an appropriate name such as **EA_PG_2**.
- **Step 6** Enter a proper description.
- **Step 7** Set the Client Type to **Expert Advisor**.
- **Step 8** Leave the IP address for the primary and secondary CTI Servers blank.
- Step 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. See Figure B-36.

Figure B-36

Logical Controller		
Logical controller ID:* 5002	Physical controller ID: ★ 5002	
Name:	* EA_PG_2	
Client type:	* Expert Advisor	
Configuration parameters:		
Description:	PG for EA	
Physical controller description:		
Primary CTI address:		
Secondary CTI address:		9107
		ន្ត្រី

After the creation of the logical controller the underlying peripheral can now be added.

- Step 1 Select the EA_PG_2 PG that was just added from the PG explorer results on the left.
- Step 2 Click Add Peripheral.
- **Step 3** Enter an appropriate peripheral name such as **EA_PG_2_1**.
- **Step 4** Select the Client Type as **Expert Advisor**.
- Step 5 Under Configuration Parameters enter /ExtendedAgent.
- **Step 6** Select the Default Desk Settings option to NONE.
- **Step 7** Enter a proper description.
- Step 8 Check the Enable post routing option.
- Step 9 Check the Peripheral auto configured option.
- Step 10 Click Save.

After clicking **Save**, the peripheral ID will be automatically generated; note it for later use when installing the peripheral gateways in ICMSetup. See Figure B-37.

Skill Group Mask Ro	outing client Defau	It route Peripheral Monitor
Peripheral	Advanced	Agent Distribution
Peripheral ID:	★ 5003	
Name:	* EA_PG_2_1	
Peripheral name:	* EA_PG_2_1	
Client type	* Expert Advisor	
Location:		
Abandoned call wait time:	* 5	
Configuration parameters:	/ExtendedAgent	
Call control variable map:		
Default desk settings:	NONE	•
Peripheral service level type	* Calculated by Call C	enter 🔽
Description:		
Enable post routing:	Peripheral a	auto configured: 🔽

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

- **Step 1** Enter an appropriate peripheral name such as **EA_PIM**.
- **Step 2** Select the Client Type as **Expert Advisor**.
- **Step 3** Select the Default media routing domain option to **NONE**.
- **Step 4** Enter a proper description.
- Step 5 Click Save. See Figure B-38.

Figure B-38

Peripheral	Advanc	ed 🗍	Agent Distributio	on
Skill Group Mask	Routing client	Default ro	ute Peripheral I	vlonitor
Name:	* EA_PI	4	ID: * 5003	
Timeout threshold:	* 5000			
Late threshold:	* 2500			
Timeout limit:	* 20			
Default media routing don	nain: NONE			•
Default call type:	NONE			•
Configuration parameters:				
Dialed Number/Label map	p: * Donot	use DN/Labe	el map	•
Client type:	* Expert	Advisor		•
Description:				
Network routing client:				
Network transfer preferred	± 🗖			

Step 6 On the Advanced tab, ensure that the Agent auto-configuration option is not checked.

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

Peripheral Gateway Installation for CUCCE

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.

Note

A single PG can support ACD PIMs, VRU PIMs, and Media Routing PIMs, though the ACD PIMs must all be of the same kind and the VRUs must all be of the same kind.

Before you install a Peripheral Gateway (PG), the Windows operating system (for version specifics refer to the Cisco Intelligent Contact Management Software Release 7.5(1) Bill of Materials—including SNMP and (for Windows 2003) 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 CallRouter, a Logger, and the Admin Workstation.

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

For each PG, you must have defined a *Logical_Interface_Controller* record, a *Physical_Interface_Controller* record, and a Peripheral record for each PIM you intend to configure--though at least one Peripheral record is necessary. (Configure ICM creates these records automatically if you choose Configure a PG using the PG Explorer.)



ICM software restricts running more than two PGs of the same instance on a single machine at the same time.

Figure B-39 shows the deployment of redundant servers with peripheral gateways.



The following section outlines the steps to install two peripheral gateways with three peripheral interface managers for the solution. More information on peripheral gateway installations and configurations can be found in the *ICM Setup and Installation Guide*.

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:

- **Step 1** Select the network **Domain** for the instance.
- **Step 2** Select the **Facility** Organizational Unit for the instance.
- Step 3 Select the Instance Name for the instance.



The ICM Instance Name is the name of the Instance Organizational Unit.

Step 4 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.

Step 5 Click OK.

Figure B-40

Cisco ICM Setup	Add Add
Upgrade All	Add Instance
Prompt for Secur	The selected facility does not contain an available ICM instance OU. Please select another facility, or use the ICM Domain Manager to add a new instance OU to this facility.
	Domain Manager

You can now add ICM Instance components.

Step 1 In the ICM Setup application, click the **Add** button on the right under **Instance Components**. See Figure B-41.

Figure B-41



- **Step 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:
 - CallManager

- VRU
- f. Click Next. See Figure B-42.

Figure	B-42
--------	------

Peripheral Gateway Properties		×
	Node Manager Properties Production mode Auto start at system startup Duplexed Peripheral Gateway Client Type Selection	PG Node Properties ID: PG 1 Side A Side B
	Available types: ACP1000 Agent Routing Services Alcatel Definity DMS100 Expert Advisor G2 Galaxy IPCC Enterprise Gateway IPCC Express Gateway	Selected types: CallManager VRU move
	Drive:	
	Help < <u>B</u> ack Nex	t> Cancel

Step 3 For the Peripheral Gateway Component Properties click Add in the Peripheral Interface Managers section. Set the Client type as CallManager and select PIM 1 from the Available PIMS List. Click OK. See Figure B-43.

Fiaure	B-43

Peripheral Gateway Component	Properties	×
	Peripheral Interface Managers	Add Edit Delete
Add PIM	Client Type: CallManager Available PIMS: PIM 2 PIM 3 PIM 4 PIM 5 Cancel Help Cancel Help Cancel Us Cancel Us	1 vanced CS Setting: EAS Mode 3-PHD Mode ing MAPD
	Help < <u>B</u> ack <u>N</u> ext >	Cancel

Step 4 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 CallManager 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. See Figure B-44.

Figuro	R-11
riyure	D-44

CallManager Configuration (PIM 1)		
Enabled		
Peripheral name:	CM_PIM_1	
Peripheral ID:	5000	
Agent extension length:	4	
- CallManager Parameters		
Service	192 168 45 182	
UserId	itapi	
User password:	*****	
Mobile Agent Codec	6 711	
OK Ca	ncel Help	A115
		8

Step 5 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. See Figure B-45.

Figure B-45

Peripheral Gateway Componer	nt Properties	×
	Peripheral Interface Managers	
	PIM 1; Enabled, PID: 5000, CallManager	Add
		Edit
		Delete
Add PIM	<u>×</u>	
	Client Type:	1
	VRU	2
	Available PIMS:	
	PIM 2	vanced
	PIM 4 PIM 5	
	PIM 6	
		CS Setting:
	Cancel Help	i EAS Mode
	C EA	S-PHD Mode
	Queue Reporting	sing MAPD
	Help < <u>B</u> ack <u>N</u> ext >	Cancel 7

Step 6 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. See Figure B-46.

Figure B-46

VRU Configuration (PIM 2)	×
Peripheral name:	VRU_PIM_2
Peripheral ID:	5001
VRU host name:	192.168.45.131
VRU Connect port:	5000
Reconnect interval(sec):	10
Heartbeat interval (sec):	5
DSCP:	CS3(24)
OK Cancel	

Step 7 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. See Figure B-47.

Peripheral Gateway Componen	t Properties	×
	– Peripheral Interface Managers PIM 1; Enabled, PID: 5000, CallM PIM 2; Enabled, PID: 5001, VRU	fanager Add Edit Delete
	Peripheral Gateway configuration- Logical controller ID: CTI Call Wrapup Data delay: Demand command server Event Link. MIS Enabled VRU Reporting Event Feed Service Control Queue Reporting	5000 0 Advanced Definity ECS Setting: Non EAS Mode EAS Mode EAS-PHD Mode Using MAPD
	Help < <u>B</u> ack !	Next > Cancel

Step 8 On the Device Management Protocol Properties set **Side A preferred** option and click **Next**. See Figure B-48.

Device Management Protocol F	Properties	X
	Side A preferred Side B preferred No side preference Side A properties CallRouter is local CallRouter is remote (WAN) Usable Bandwidth (Kbps): Bandwidth (Kbps): Side B properties CallRouter is local CallRouter is remote (WAN) Usable Bandwidth (Kbps): Side B properties CallRouter is remote (WAN) Usable Bandwidth (Kbps): Side B properties Side A properties Side B properties Side B properties Side A properties	
Help	< Back Next > Cancel	

Step 9 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**. See Figure B-49.

228119

Peripheral Gateway Network In	nterfaces		×
	Private Interfaces:		
	PG private A:	192.168.9.21	
	PG private A high:	192.168.9.21	
	PG private B:	192.168.9.22	
	PG private B high:	192.168.9.22	QoS
	Visible Interfaces:		
57	PG visible A:	192.168.45.151	
	PG visible B:	192.168.45.152	
	Router visible A:	192.168.45.141	
N HY	Router visible A high:	192.168.45.141	
	Router visible B:	192.168.45.142	
	Router visible B high:	192.168.45.142	QoS
Help	< <u>B</u> ack <u>N</u> e	xt > Cancel	

Figure B-49

Figure B-48

Step 10 Review the PG setup information and click Next to complete installation of the first PG. The ICM interface will return to the ICM Setup application, click the Add button on the right under "Instance Components" to add the second peripheral gateway. See Figure B-50.



- **Step 11** 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 2 and select the appropriate side for duplexed installations.
 - e. Select the Expert Advisor client type from the list of available types and click the Add button.
 - f. Click Next. See Figure B-51.

Figure B-51

Peripheral Gateway Properties		×
	Node Manager Properties Production mode Auto start at system startup Duplexed Peripheral Gateway	PG Node Properties ID: PG 2 © Side A © Side B
	Client Type Selection Available types: ACP1000 Agent Routing Services Alcatel Aspect CallManager Definity DMS100 G2 G2 Galaxy IPCC Enterprise Gateway IPCC Express Gateway	Selected types: Expert Advisor
	Drive:	
	Help < <u>B</u> ack <u>N</u> ex	Cancel

Step 12 For the Peripheral Gateway Component Properties click Add in the Peripheral Interface Managers section. Set the Client type as Expert Advisor and select PIM 1 from the Available PIMS List. Click OK. See Figure B-52.

<u>Note</u>

The number of PIMs is only significant within the respective PG. If you have only a few PGs deployed with few PIMs, it is acceptable to assign PIMs that match the PG numbering for ease of documenting.

Figure B-52

Peripheral Gateway Componen	t Properties	×
	Peripheral Interface Managers	
	Add	
	Edit	
	Delete	i I
	X	
	Client Type:	
	Expert Advisor	
	Available PIMS:	
	PIM 1 vanced	
	PIM 3 PIM 4	
	PIM 5	
	ECS Setting:	
	Cancel Help TEAS Mode	
	C EAS-PHD Mode	
	Queue Reporting Using MAPD	
		<u> </u>
	Help < <u>B</u> ack <u>N</u> ext> Cancel	

Step 13 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. Enter the IP address or name of the Expert Advisor Runtime Server.
- e. Accept the default Expert Advisor server port or enter a different one as configured.
- f. Click OK. See Figure B-53.

Figure B-53

Expert Advisor Configuration (PI	M 1) 🔀
Enabled	
Peripheral name:	EA_PIM_1
Peripheral ID:	5003
Expert Agent Runtime Server name:	192.168.81.101
Expert Agent Runtime Server port:	42067
OK Cancel	Help

Back on the Peripheral Gateway Component Properties, enter the Peripheral Gateway Logical controller ID that was generated for the Expert Advisor PG by the Configuration Manager on the Admin Workstation and then click **Next**. See Figure B-54.



Peripheral Gateway Componen	t Properties	×			
	Peripheral Interface Managers				
	PIM 1; Enabled, PID: 5003, Exp	ert Advisor Edit Delete			
	- Peripheral Gateway configuration				
	Logical controller ID:	5002			
57	CTI Call Wrapup Data delay:	0			
	Demand command server				
	🗖 Event Link	Advanced			
	MIS Enabled				
V A	VRU Reporting	Definity ECS Setting:			
	C Event Feed	C Non EAS Mode			
	C Service Control	C EAS Mode			
	🗖 Queue Reporting	C EAS-PHD Mode			
	Help < <u>B</u> ack	Next > Cancel			

Step 14 On the Device Management Protocol Properties set Side A preferred option and click Next. See Figure B-55.

Figure	R-55
inguic	200

Device Management Protocol Properties	×
 Side A preferred Side B preferred No side preference Side A properties CallRouter is local CallRouter is remote (WAN) Usable Bandwidth (Kbps): [30000 Heartbeat Interval (100ms): 4 	
Side B properties CallRouter is local CallRouter is remote (WAN) Usable Bandwidth (Kbps): 30000 Heartbeat Interval (100ms):	
Help < <u>B</u> ack <u>N</u> ext > Cancel	

Step 15 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**. See Figure B-56.

Figure B-56

Peripheral Gateway Network 1	Interfaces		×
	Private Interfaces:		
	PG private A:	192.168.9.21	
	PG private A high:	192.168.9.21	
	PG private B:	192.168.9.22	
	PG private B high:	192.168.9.22	QoS
	Visible Interfaces:		
57	PG visible A:	192.168.45.151	
	PG visible B:	192.168.45.152	
	Router visible A:	192.168.45.141	
NL NT	Router visible A high:	192.168.45.141	
	Router visible B:	192.168.45.142	
	Router visible B high:	192.168.45.142	QoS
Help	< <u>B</u> ack <u>N</u> e	xt> Cancel	

Step 16 Review the PG setup information and click **Next** to complete installation of the PG.

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 device's 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.

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. See Figure B-57 and Figure B-58.

abab	Cisco Unifie	d CM Adm	inistrati	on					Navigation 🧕	Cisco Unified	CM Admi	nistration 👻	Go
cisco	For Cisco Unified	Communication	s Solutions							bmcal	oth I A	bout Lo	aout
vstem 👻	Call Routing - Med	lia Resources 👻	Voice Mail 👻	Device 👻	Application	n 🛩 User Mar	agement 👻	Bulk Adr	ninistration 👻	Help 👻			
		_	_			_		_	_		_	_	
ind and l	List Plugins												
Status —													-1 ⁻
i 12 re	cords found												
Plugin	(1 - 12 of 12)									Ra	ws per Pa	age 50 👻	
Find Plugir	where Name	▼ begins with	•		and Plu	gin Type equ	als Insta	llation	▼ Find	Clear Filte	er 🕂		
	Plugin Name 🕈					D	escription						
<u>Download</u>	Cisco CTL Client	This plugin rel updates the fi MD5(/usr/loca d9:0f:41:41:b	rieves the C le on the Cis l/thirdparty/j 6:a1:ac:d4:	TL file from sco TFTP serv jakarta-tomo 2a:18:bd:7c	the Cisco ver. at/webapp dd:d3:27	TFTP server. os/plugins/Cis 7:0b	It digitally coCTLClie	signs the nt.exe)=	CTL file by	using a secur	ity token	and then	
<u>Download</u>	<u>Cisco</u> CallManager AXL SQL Toolkit	Cisco CallMan results. Comn client system. MD5(/usr/loca ce:30:0c:57:9	ager AXL SQ nunicates wit l/thirdparty/j a:94:38:4b:	L Toolkit, a z h the AXL int jakarta-tomc :5b:8a:48:21	zip file tha terface of :at/webapp b:19:5a:0	t contains a the CallMana os/plugins/ax 8:76	lava-based ger. Includ Isqltoolkit.	d toolkit fo des a sam .zip)=	or sending a ple SQL file	nd receiving and instruction	SQL state ons for ex	ments and ecuting on a	
<u>Download</u>	<u>Cisco IP Phone</u> Address Book Synchronizer	Cisco IP Phon Address Book MD5(/usr/loca ac:81:36:54:3	e Address Bo The Synchr l/thirdparty/j 31:e6:a0:93	ook Synchror onizer provid jakarta-tomc :fc:af:47:b1	nizer allow des two-wa at/webapp :4b:fb:a1:	s users to syr y synchroniza s/plugins/Ta b6	nchronize I ntion betwe bSyncInsta	Microsoft V een the Mi all.exe)=	Vindows Add crosoft and	ress Book wit Cisco product	th Cisco P :s.	ersonal	Ξ
<u>Download</u>	<u>Cisco JTAPI for</u> <u>Linux</u>	Install this plu standard prog documentation MD5(/usr/loca 19:f9:76:c4:2	igin on all co ramming int n and sampl l/thirdparty/j 0:71:55:d3:	mputers tha erface for tel le code are ir jakarta-tomc :36:8f:25:33	at host app lephony ap ncluded. T :at/webapp ::9e:cf:6b:	plications that pplications wr his plugin is os/plugins/Cis 2f	interact w itten in the meant for coJTAPIC	ith Cisco C a Java pro Linux plat ient-linux.	CallManager gramming la forms. bin)=	via JTAPI. JT anguage. JTA	API provi PI referen	des the nce	
<u>Download</u>	<u>Cisco JTAPI for</u> <u>Solaris Sparc</u>	Install this plu standard prog documentation MD5(/usr/loca bd:9f:05:e6:4	igin on all co ramming int n and sampl l/thirdparty/j 0:d7:c1:94:	mputers tha erface for tel le code are ir jakarta-tomc :a4:b5:93:ef	at host app lephony ap ncluded.Th at/webapp f:6e:0e:f1	plications that pplications wr his plugin is n ps/plugins/Cis :10	interact w itten in the neant for S coJTAPIC	ith Cisco C a Java pro Solaris Spa ient-solari	CallManager gramming la irc platforms sSparc.bin)=	via JTAPI. JT anguage. JTA -	API provi PI referen	des the nce	
<u>Download</u>	Cisco JTAPI for Solaris X86	Install this plu standard prog documentation MD5(/usr/loca bd:9f:05:e6:4	igin on all co ramming int n and sampl l/thirdparty/j 0:d7:c1:94:	mputers tha erface for tel le code are ir jakarta-tomc :a4:b5:93:ef	at host app lephony ap ncluded.Th at/webapp f:6e:0e:f1	plications that pplications wr his plugin is n os/plugins/Cis :10	interact w itten in the neant for S coJTAPICI	ith Cisco C a Java pro Solaris X86 ient-solari	CallManager gramming la platforms. sX86.bin)=	via JTAPI. JT anguage. JTA	API provi PI referei	des the nce	
Download	Cisco JTAPI for Windows	Install this plu standard prog documentation MD5(/usr/loca 77:6e:6d:e5:0	igin on all co ramming int n and sampl l/thirdparty/j :1:4f:b5:e0:	mputers tha erface for tel le code are in jakarta-tomc :a7:85:bf:02	at host app lephony aj ncluded. T :at/webapp !:aa:d1:c7	plications that pplications wr his plugin is ps/plugins/Cis :c9	interact w itten in the meant for coJTAPIC	ith Cisco C e Java pro Windows p ient.exe)=	CallManager gramming la blatforms.	via JTAPI. JT anguage. JTA	API provi PI referen	des the nce	
<u>Download</u>	<u>Cisco TAPS for</u> <u>Windows</u>	Cisco Tool for a machine with MD5(/usr/loca ee:36:e2:17:	Auto-Regist h a version o l/thirdparty/j 10:62:6a:c9	ered Phone S of CRS that is jakarta-tomc 181:e3:0b:5	Support (T s compatit at/webapp d:9c:59:73	APS) loads a ble with the C bs/plugins/To 3:cd	preconfigi isco Unifie olforAutoR	ured phon d CallMan egisteredi	e setting on ager version PhonesSupp	a phone. In: ort.exe)=	stall this o	component o	'n
<u>Download</u>	<u>Cisco Telephony</u> <u>Service Provider</u>	This product of CallManager s CallManager s Windows oper the Cisco TSP Solution. MD5(/usr/loca	ontains the (erver or on a erver via TC ating system and the Cisc l/thirdpartv/i	Cisco TAPI se any other con :P/IP. TAPI, a n. The Cisco co Wave Driv jakarta-tomc	ervice prov mputer tha a standard TAPI Deve vers to allo :at/webapp	vider (TSP) ar at is running l programmin eloper's Guide ww TAPI applic ps/plugins/Cis	nd the Cisc a Microsoft g interface describes ations to r coTSP.exe	to Wave D t Windows for telepl the TAPI make and e)= 77:ae	rivers. Insta operating s hony applica interfaces tl receive calls :64:b0:5c:2	II the applica ystem that in tions, runs o hat are curren s on the Cisco a:24:a1:d5:8	tion on th teracts wi n the Mice htly suppo o IP Telep 3b:2d:a3:	e Cisco th the Cisco osoft orted. Install ohony 21:11:0a:22	2
Download	Cisco Unified CM	Cisco Unified	CallManager	Serviceabilit	y Real-Tin	ne Monitoring	Tool, a cl	ient tool, i	monitors rea	al-time behav	ior of the	component	5 7
one							/ Trusted	sites Prot	ected Mode:	Off	- @ -	95%	-

🚟 icm1-PG1A jtapigw - jgw1 - [ACTIVE]
00:29:33 Trace: Calling getProvider(> 192.168.93.100;login=jtapi;passwd=<***edit
00:29:51 Trace: Returned successfully from getProvider()
00:29:51 Trace: disableAll() TraceManager for CTICLIENT
00:29:51 Trace: Waiting for the provider to be in service 🗾
00:29:51 Trace: ProvOutOfServiceEv
00:29:51 Trace: ProvInServiceEv
00:29:51 Trace: Provider is in service
00:29:51 Trace: Successfully configured JTAPI Object.
00:29:51 Trace: [Thread-1]ThreadAddressManager ends adding observers after 0 mil
00:29:51 Trace: Creating server socket on port 40029 to listen for PIM connectio
00:29:51 Trace: ThreadAddressManager::processNextQueuedMsg: msgHashtable.size =
00:29:51 Trace: ThreadAddressManager::Waiting for next retry
00:30:29 Trace: PIMServer: Accept connection only to loopbackaddress_127.0.0.1/1
00:30:29 Trace: PIMServer: Accepted connection from 127.0.0.1/127.0.0.1
00:30:29 Trace: PIMServer: hostaddress 127.0.0.1/127.0.0.1
00:30:30 Trace: MsgOpenReq: InvID: 7425968 Ver: 2 IdleTimeout: 80000
00:30:30 Trace: Initializing PIM Connection
00:30:30 Trace: Successfully initialized PIM Connection.
00:30:30 Trace: Adding Address Observers to all CTI Addresses
00:30:30 Trace: [Thread-1]ThreadAddressManager ends adding observers after 0 mil
00:30:30 Trace: ThreadAddressManager::processNextQueuedMsg: msgHashtable.size =
00:30:30 Trace: ThreadAddressManager::Waiting for next retry
00:30:30 Trace: MsgOpenConf: InvID: 7425968
00:35:47 Trace: JUM Total Memory: 33423360 JVM Free Memory: 32899760 JVM Heap in

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

CTI Server Installation

The CTI Server is an optional ICM node that allows a desktop or server application to receive call control information from the ICM and from call center peripherals. This information can be used, for example, in a screen pop on the agent's desktop. The CTI Gateway is available as part of the Cisco Enterprise CTI product.



Cisco supports installation of CTI Server on the same machine where the Peripheral Gateway software is installed. Installing CTI Sever 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. Logically, it can be viewed as shown in Figure B-59.



Figure B-59 CTI Communication



Figure B-60



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:

- **Step 1** Check the **Production node**.
- **Step 2** Check the **Auto start at system startup**.
- **Step 3** Check the **duplexed** Peripheral Gateway.
- Step 4 Set the CG Node Properties ID to CG 1 and select the appropriate side for duplexed installations.
- Step 5 Click Next. See Figure B-61.

Eiguro	P 61
Figure	B-0 I

CTI Server Properties	×
	Node Manager properties Image: Production mode Image: Auto start at system startup Image: Duplexed CTI Server CG node properties ID: Image: CG 1 ID: Image: CG 1 ICM system ID: 1 ICM system ID: 1 Image: Side A Image: Side B Drive: Image: Comparison Start Star
Help	< <u>B</u> ack <u>N</u> ext > Cancel

Step 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**. See Figure B-62.

Figure B-62

- CTI Server configuration -			
	Client Connection Port Number:	42027	2
	Agent Login Required for Cli	ent Events	22815

Step 7 Configure the PG and CG Public and Private interfaces. Click **Next**. See Figure B-63.

CTI Server Network Interface Pr	operties	×
	PG private interfaces	
	Node A:	192.168.9.21
	Node B:	192.168.9.22
	CG private interfaces	
	Node A:	192.168.9.21
	Node B:	192.168.9.22
	CG visible interfaces -	
	Node A:	192.168.45.151
	Node B:	192.168.45.152
y all		
Help	< <u>B</u> ack	Next > Cancel

Step 8 Review the CG setup information and click **Next** to complete installation of the CTI Gateway.

CTIOS Server Installation

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. http://www.cisco.com/en/US/partner/products/sw/custcosw/ps14/prod_installation_guides_list.html

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.

- **Step 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.
- Step 2 Under the CTI OS Instance List, click Add.
- **Step 3** Enter an instance name (e.g., "ctios").
- Step 4 Now click on Add inside the CTI OS Server List. The Add CTIOS Server dialog appears.

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.

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. See Figure B-64 and Figure B-65.



Fiaure	B-65
riguio	000

CTI Server Information	x	
	Instance Name ctios CTIOS Server Name CTIOS1	
	System <u>A</u> Name or IP Address: [192.168.45.151 Port: 42027	
	System B Name or IP Address: 192.168.45.152 Port: 42027	
Help	< <u>B</u> ack <u>N</u> ext > Cancel	228136

Step 5 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. See Figure B-66.

Figure B-66

Peripheral Identifier		×
	Peripheral ID and Peri configured in the CTI S	pheral Type as Server are required:
	Instance Name	ctios
	CTIOS Server Name	CTIOS1
	Logical Name:	IPCC1
	<u>P</u> eripheral ID:	5000
	Peripheral <u>T</u> ype:	IPCC 💌
	Login By Agent ID Login Name	
	🔽 Enable Mobile	Agent
	Mobile agent mode	Agent chooses
Help	< <u>B</u> ack	Next > Cancel

Step 6 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. See Figure B-67.

gure B-67			
onnection Information			×
	Enter the port number a for the CTIOS Server In	and heartbeat information Istance	
	Instance Name	ctios	
	CTIOS Server Name	CTIOS1	
	Listen Port	42028	
	Heartbeat Retry	5	
	Heartbeat Interval	60000	
Help	< <u>B</u> ack N	ext > Cancel	6138
			- R

Fi

C

Enter the default polling interval for Skillgroup statistics (in seconds). Click Next. See Figure B-68. Step 7

Figure B-68

Statistics Information		×
	Instance Name CTIOS Server Name CAD Agent CAD Agent Polling for Agent Statistics Polling Interval for Agent Statistics (seconds) Polling Interval for Skillgroup Statistics (seconds) Enable Quality of Service In order for CTIOS to have fu also enable QoS during instat to this server. NDTE: Enabling QoS will DIS information, see the System M	ctios CTIOS1 s at End Call 0 10 (QoS) Illy functional QoS, you must illation of all clients connecting SABLE STATISTICS. For more Manager's Guide.
Help	< <u>B</u> ack	Next > Cancel

Step 8 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. See Figure B-69.

1 14416 0-03

eer CTIOS Server	Duplex CTIOS Install Enter the name (or tcp/ip address) and port number of the other CTIOS server in the duplex configuration. (If there are more than 1 configured those listed after the 1st will be
	deleted.): Instance Name ctios
	CTIOS Server Name CTIOS1
	Peer CTIOS Server: 192.168.45.152
	Port: 42028
<u>H</u> elp	< <u>B</u> ack <u>F</u> inish Cancel

Step 9 The Security installation is launched with the dialog shown in Figure B-70.

Figure B-70

Cisco CTIOS Server Security	×
A mix of secure and non-secure CTIC security is enabled, CTIOS clients wil secure mode.	DS clients is not allowed. If I automatically operate in
WARNING: Once security is enabled clients will no longer be able to connu using .NET CIL or Java CIL.	d, CTIOS 6.0 and earlier ect, nor will CTIOS clients
Enable Security	
Self Signed Certificate Authori	à
C Third Party Certificate Authority	y
CTIDS Server Certificate Password:	
Peer Server Certificate Password:	
Monitor Mode Password:	
InstallShield	
	Ok Cancel

Step 10 If you wish to disable Security, just click OK; otherwise, check the checkbox and enter the appropriate information, and click OK. For more information about CTI OS Security, see Chapter 7, "CTI OS Security" in the CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions Guide.

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.

Create Device Target in Configuration Manager

Create each of the Device Targets using the following steps:

- **Step 1** Open the Configurations Manager on the AW.
- **Step 2** Select the **Device Target Explorer** option under the **Tools > Explorer Tools** group.
- Step 3 Click Retrieve.
- Step 4 Click Add Device Target.
- **Step 5** Enter an appropriate name such as the agent Extension "6001".
- **Step 6** Enter the Global Address, also the extension number for fully qualified number.
- Step 7 Enter the Configuration parameters as follows "/devtype CiscoPhone /dn 6001".
- **Step 8** Enter a description if desired.
- Step 9 Then Click Save. See Figure B-71.

Select filter data	Device target	
	Name: * 6001	
Optional Filter Condition Value	Global address: * 6001	
None	Configuration parameters //devtype CiscoPhone /dn 6001	
Save <u>Retrieve</u> Cancel filter changes	Description:	
▼ Hide legend	Label	
(1) Device target	Routing client: * CUCM_RC	-
(2) Labei	Label: * 6001	
	Label type: * Normal	•
Xick on an item to edit or view its contents. Ise the Add buttons to create new items.	Customer: icm	•
⊡	Description:	
EVEN 6001.CUCM_RC		
6006 CUCM BC		
5006.CVP_VRU_PIM		
■		
6102.CVP_VRU_PIM		
6103.CUCM_RC		
UNASSIGNED		
-		
% (2) Add Label Multiple		
	Save Close	<u>H</u> elp

- **Step 10** Add label for each of the routing-clients. In this setup there are the following two routing clients:
 - CU Communication Manager

• CU CVP VRU

These two routing clients can request for labels from CUICM and CUICM will return the label to the routing-client. Figure B-72 shows a label for CUCM Routing Client.

Fiaure	B-72

Device target				
Name:	*[6001		
Global address:	*[5001		
Configuration parameters	- [/devtype CiscoPhone /dn 6001		
Description:	Γ			
	_			
Label				
Routing client:	*	CUCM_RC	7	
Label:	*	6001		
Label type:	*	Normal	•	
Customer:		icm	•	0,
Description:				22814

Figure B-73 shows a label defined for CVP Routing Client.

Figure B-73

Device target	
Name: *	6001
Global address:	6001
Configuration parameters	/devtype CiscoPhone /dn 6001
Description:	
Label	
Routing client:	CVP_VRU_PIM
Label:	* 6001
Label type:	* Normal
Customer:	icm 🔽
Description:	

Network VRU Configuration in AW Configuration Manager

Create the Network VRU device as follows:

Step 1 Open the Configurations Manager on the AW.

Step 2 Select the Network VRU Explorer option under the Tools > Explorer Tools group.

Step 3 Click Retrieve.

- Step 4 Click Add Network VRU.
- **Step 5** Enter an appropriate name such as "**cvp**".
- **Step 6** Select the type as "**Type 10**".
- Step 7 Enter a description such as the extension numbers associated with CVP and the VXML Gateway.
- **Step 8** Then Click **Save**. See Figure B-74.

Figure B-74

Network VRU	Network VRU Banks
Name:	* CVE
Туре:	* Type 10
Description:	CCenter # 1005-6

After the Network CVP VRU is created, add labels for each of the Route Clients as follows:

- Step 1 Click Add Label.
- **Step 2** Select the Network VRU **cvp**.
- **Step 3** Select the Route Client **CUCM_RC**.
- **Step 4** Enter the label of the CVP Extension line **1005**.
- **Step 5** Select **normal** for the label type.
- **Step 6** Select **icm** as the Customer.
- **Step 7** Enter a description as desired.
- Step 8 Click Save. See Figure B-75.

Figure B-75

Label		
Network VRU:	сур	•
Routing client:	* CUCM_RC	~
Label:	* 1005	
	1	
Label type:	* Normal	•
Label type: Customer:	* Normal	•
Label type: Customer: Description:	* Normal icm	•

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

228146

- Step 1 Click Add Label.
- **Step 2** Select the Network VRU **cvp**.
- **Step 3** Select the Route Client **CVP_VRU_PIM**.
- **Step 4** Enter the label of the CVP Extension line **1006**.
- **Step 5** Select **normal** for the label type.
- **Step 6** Select **icm** as the Customer.
- **Step 7** Enter a description as desired.
- Step 8 Click Save. See Figure B-76.

🚯 Network ¥RU Explorer			
_Select filter data	Network VRU Netw	work VRU Banks	
	Name:	* cvp	
Optional Filter Condition Value	Туре:	* Type 10	•
	Description:	CCenter # 1005-6	
Hide legend			
(ⓓ) Network VRU └──छ (2) Label			
Click on an item to edit or view its contents. Use the Add buttons to create new items.			
	Label		
	Network VRU:	сур	
	Routing client: Label:	* CVP_VRU_PIM * 1006	<u> </u>
	Label type:	* Normal	-
	Customer:	icm	_
	Description:		
2 Add Label Delete Multiple			
		<u>S</u> ave <u>C</u> lose	
CM Instance: icm			000

Step 9 After the network VRUs have been created, add a Contact Center Agent and Skill Group for testing purposes.

Add Agents

Create the Agent as follows:

- **Step 1** Open the Configurations Manager on the AW.
- **Step 2** Select the **Agent Explorer** option under the **Tools > Explorer Tools** group.
- Step 3 Click Retrieve.
- Step 4 Click Add Agent.
- **Step 5** Enter an appropriate first, last, and login name.
- **Step 6** Enter an appropriate password.
- **Step 7** Verity the Enterprise name that was generated is appropriate.
- **Step 8** Enter an AgentID number or allow one to be generated automatically. This number is used during agent login to the Agent desktop client.
- **Step 9** On the Supervisor tab, check **Supervisor agent** if desired.
- Step 10 Click Save. See Figure B-77.

🚯 Agent Explorer	
Select filter data	Accest Advanced Chill many much which Committee
Peripheral CCM_PIM_1	Personal information First name: * bart
Optional Filter Condition Value None Save Retrieve Cancel Filter changes	Last name: ★ mcglothin Login name: ★ bmcgloth Password:
	Enterprise name: * Generic_CCM_PG_1.mcglothin_bart
Hide legend I) Agent I2) Route I3) Peripheral target	Peripheral name: AgentID (Peripheral number): * 9001 (value will be created if left blank)
E (4) Label	
Click on an item to edit or view its contents.	
Generic_CCM_PG_1.mcglothin_bert UNASSIGNED	
2 (1) Add Agent Multiple	
G(j) (2) Add Route	Save Lep c
ICM Instance: icm	

Add Skill Group

Create a Skill Group as follows:

- **Step 1** Open the Configurations Manager on the AW.
- **Step 2** Select the **Skill Group Explorer** option under the **Tools > Explorer Tools** group.
- Step 3 Click Retrieve.
- Step 4 Click Add Skill Group.
- **Step 5** Enter a Peripheral name such as **PreSale**.
- **Step 6** Enter an appropriate Name such as **Generic_Presale**.
- **Step 7** Select the Media Routing domain **Cisco_Voice**.
- **Step 8** On the Skill Group Members tab click add and select the agent created earlier.
- Step 9 Click Save.
- **Step 10** Add route option in the skill group.
- Step 11 Click Add Route.
- Step 12 Assign an appropriate name such as Generic_PreSale_Route.
- Step 13 Click Save. See Figure B-78.

Fiaure	B-78
gaio	

Select likel data	
Peripheral CCM_PIM_1	Skill Group Members Subgroup Mask Sub skill groups Skill Group Advanced Media routing domain: * Cisco_Voice • Peripheral number: 0 Peripheral name:* PreSale Name: * Generic_Presale • • Available holdoff delay (sec): Use Peripheral Default Priority 0 Extension: ICM picks the agent • Route Skill group priority: 0 • Name: * Generic_PreSale_Route • • Description • • • Service name: NONE • •

Step 14 The next step is to create Call Type Lists for the Presales group and the Expert Advisor Service.

Add Call Type List

Create a Call Type List as follows:

Step 1	Open the Configurations Manager on the AW.
Step 2	Select the Call Type List option under the Tools > Explorer Tools group.
Step 3	Click Retrieve .
Step 4	Click Add.
Step 5	Enter a name such as PreSales_SanJose or Expert_Advisor_Service .
Step 6	Select the Customer icm .
Step 7	Enter an appropriate description as desired.
Step 8	Click Save. See Figure B-79.
Step 9	Repeat for second list.

🛱 Call Type List			
Select filter data	Attributes		
Customer (All>	Name	* Expert_Advisor_Service	
Optional Filter Condition Value	Call Type ID	* 5001	
None	Customer	icm	
Save <u>Retrieve</u> Cancel filter changes	- Service level		
Call Type			Override System Information Default
Expert_Advisor_Service PreSales_SanJose	Service level threshold	20	
	Service level type	Ignore Abandoned Calls	
			Override System Information Default
	Bucket intervals	Default_Bucket_Intervals	
	Description		
Add Delete Revert		Save	<u>C</u> lose <u>H</u> elp
ICM Instance: icm			

Add Dialed Number/Script Selector List

Create a Dialed Number List as follows:

Step 1	Open the Configurations Manager on the AW.
Step 2	Select the Dialed Number/ Script Selector List option under the Tools > Explorer Tools group.
Step 3	Click Retrieve .
Step 4	Click Add.
Step 5	Select the Routing client CUCM_RC.
Step 6	Select the Media routing Domain Cisco_Voice.
Step 7	Enter the Dialed Number string that is called to reach this queue.
Step 8	Enter a name such as CUCM_RC.1000 or CUCM_RC.1301 as appropriate.
Step 9	Select the Customer icm .
Step 10	Leave the default Label as <none></none> .
Step 11	Enter an appropriate description as desired.

Cisco Virtual Expert Management for Retail Design and Implementation Guide

- Step 12 Click Save. See Figure B-80.
- **Step 13** Repeat for additional dialed numbers.

Select filter data			Attributes Dialed Number Mapping D	ialed Number Label	
Routing client	<all></all>		Routing client	*CUCM_RC	Ŧ
Customer	<all></all>		Media routing domain	* Cisco_Voice	•
None	Londition Value		Dialed number string / Script selector	* 1301	
Save	<u>R</u> etrieve Car	ncel filter changes	Name	* CUCM_RC.1301	
aled Number / Script Selecto	ı		Customer	icm	•
Name CUCM RC.1000			Default label	<none></none>	•
CUCM_RC.1301			Description		
			Permit application routing		
			Reserved by IVR		

Figure B-80

Step 14 On the Dialed Number Mapping Tab, select the calling line ID, Caller Entered digits (if any) and the Call type. For the 1301 dialed number the Expert_Advisor_Service was selected, for the 1000 dialed number PreSaled_SanJose was selected. See Figure B-81.



- :	D 04
Figure	B-81

Calling Line ID	
© All	
C Region Dialed Number Mapping Dialed Number Label	
C Prefix CLID / App String 1 CED / App String 2 Call type	ſ
C Match All All Expert_Advisor_Service	
Called-entered digits	
© All	
O None	
Required	
Entered	
O CED	
Call type Expert_Advisor_Service	
OK Cancel Help Add Edit Remove Up Down	228152

Enable Expanded Call Context

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

- **Step 1** Open the Configurations Manager on the AW.
- **Step 2** Select the **System Information** option under the **Configure ICM > Enterprise > System Information** group.
- Step 3 Check the Expanded call context option.
- Step 4 Click Save. See Figure B-82.

System Information		
General		Call T
ICM type	Standard	Defa
Company name	icm	Abar
Controller domain name	cisco-irn.com	Sorr
Partitioning enabled		3614
Maximum partitions	0	Servi
Expanded call context en	abled	Buck
- Script		CLID ម្ន័
Retain script versions	All	

Installing the Admin Workstation

CUICM Instance Explorer Setting

An additional customer definition must be created for CVP under the ICM instance. Create a customer definition as follows:

- **Step 1** Open the Configurations Manager on the AW.
- **Step 2** Select the **ICM Instance Explorer** option under the **Tools > Explorer Tools** group.
- Step 3 Click Retrieve.
- **Step 4** Select the desired instance.
- Step 5 Click Add Customer definition.
- **Step 6** Enter an appropriate name.
- **Step 7** Select the Network VRU as **cvp**.
- **Step 8** Enter an appropriate description as desired.
- **Step 9** Click **Save**. See Figure B-83.

ICM Instance Explorer	
Select filter data	ICM Instance ICM Node
	Name: * icm
Optional Filter Condition Value	Type: * Standard
None	Instance number * 0
Save <u>R</u> etrieve Cancel filter changes	Network ICM instance
	Description:
Hide legend	
1) ICM Instance	
(2) Lustomer derinition	
Click on an item to edit or view its contents. Use the Add buttons to create new items.	
2 icm	
	Customer definition Customer options
	Name: * Icm
	Description:
	Feature control set: NONE
2 (2) Add Customer definition Delete Multiple	
	Save Dise Heb
M Instance: icm	

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:

- **Step 1** Open the Configurations Manager on the AW.
- Step 2 Select the Expanded Call Variable List option under the Tools > Explorer Tools group.
- Step 3 Click Retrieve.
- Step 4 Click Add.
- **Step 5** Using the table of information below, configure each variable.
- **Step 6** Enter the variable name.
- **Step 7** Set the variable maximum length.
- **Step 8** If an array size is defined, check the array option and set the size.
- **Step 9** Set the variable as enabled.
- **Step 10** Set as persistent if specified.
- **Step 11** Enter an appropriate description as desired.
- Step 12 Click Save. See Figure B-84.
- **Step 13** Repeat for each call variable.

Table B-1 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	

Table B-1 Expanded Call Variables (continued)

1		Yes
1		Yes
40		Yes
40		Yes
10		Yes
210	1	Yes
131		Yes
1	1	Yes
1		Yes
40		Yes
	1 1 40 40 10 210 131 1 1 40	1 1 1 40 40 40 10 1 210 1 131 1 1 1 40 40

Figure B-84

Select filter data	Attributes	
	Name * user.cvpmovies_bg_media	
Optional Filter Condition Value	Maximum length * 40	
None		
Save <u>R</u> etrieve Cancel filter char	ges Maximum array size	
xpanded Call Variable		
Name	Enabled 🔽	
user.cvpmovies_bg_media vuser.h323.rftransfer	A Persistent	
🖌 user.media.id	Cisco provided	
user.microapp.caller_input	Description	
🕑 user.microapp.charset		
vser.microapp.cvpmovies_params		
vser.microapp.error_code		
vser.microapp.prome.xvz.ml		
vser.microapp.inline_tts		
user.microapp.input_type		
vser.microapp.locale		
vser.microapp.media_server		
Ver user.microapp.metadata		
vser microapp.ovende_ci		
v user.microapp.pa_ks		
vser.microapp.recording		
🖌 user.microapp.sys_media_lib		
🕑 user.microapp.ToExtVXML		
🕑 user.microapp.uui		
user.microapp.UseVXMLParams		
🕑 user. sip. refertransfer	<u> </u>	
Add Delete Revert		1

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 following scripts for use later in the Script Editor.

Create the VRU Scripts as follows:

- **Step 1** Open the Configurations Manager on the AW.
- Step 2 Select the Network VRU Script List option under the Tools > Explorer Tools group.
- Step 3 Click Retrieve.
- Step 4 Click Add.
- **Step 5** Using the table of information below, create each of the VRU Scripts.
- **Step 6** Enter the script name.
- **Step 7** Set the Network VRU as **cvp** for all entries.
- **Step 8** Enter the VRU script name.
- **Step 9** Enter the Timeout length.
- **Step 10** Enter the Configuration param.
- **Step 11** Set the Customer as **icm**.
- **Step 12** Enter an appropriate description as desired.
- Step 13 Click Save.See Figure B-85.
- **Step 14** Repeat for each Network VRU Script in the table.

Table B-2

Name	VRU Script name	Timeout	Config. Param	Int	Ovr
agentbusy	PM,agentsbusy	180			
get4digits	GD,enter_4_digits,A	180	4,4		
holdmusic	PM,holdmusic	600		у	Y
playdigits	PD,Char	180		у	
playpromptVar7	PM,-7	180		у	
requery_busy	PM,requery_busy	180			
requery_connect_failure	PM,requery_connect_failure	180			
requery_rna	PM,requery_rna	180			

Figure B-85

Network VRU Script List					_ 🗆 ×
Select filter data	Attributes				
Network VBU <all></all>		*			
Customer <all></all>	Name	get4digits			
Optional Filter Condition Value	Network VRU	* cvp		•	
None	VRU script name	* GD,enter_4_digits,A			
Save <u>R</u> etrieve Cancel filter changes	Timeout	* 180 seconds			
Network VRU Script	Configuration param	4.4			
Name	Customer	icm		-	
gentbusy get4digits	Interruptible				
Image: Market And	Overridable				
playpromptVar7	Description				
I requery_busy I requery_connect_failure					
I∎ requery_ma					
Add <u>D</u> elete Heyert			Save	Close	Help

CTI Toolkit Agent Desktop Client Installation

For Agents located in Contact Centers, or agents that would service more standard call center queues; the cisco Agent Desktop facilitates access to the queue and the tools necessary to track and monitor queue status.

The Cisco agent desktop is installed by running the Setup.exe program on the CTI disc (i.e., **D:\ctios_builds\Release\ctios\Installs\CTIOSClient**).

After running Setup.exe, complete the following steps are complete:

- Step 1 Click Next, to continue.
- **Step 2** Click **Yes** on the confirmation page.
- **Step 3** Select the Installation drive.
- Step 4 Click Next.
- Step 5 Select the Agent Desktop feature.
- Step 6 Click Next.
- **Step 7** Enter the CTIOS Server information.
- **Step 8** Enable QoS as desired.

- Step 9 Click Next.
- Step 10 If the formal agents are also using video endpoints select Enable for CVP Video.
- Step 11 Click Next.
- **Step 12** Verify installation items and click **Next**.
- Step 13 Once the installation is complete you will need to enter a CTIOS Client Certificate password between 8 and 30 characters long to secure communication between the Agent desktop and the CTIOS Server. Click OK.
- Step 14 Review the Important Note content and click Next to install security compontes.
- **Step 15** Once the client security setup is complete click **Finish**.
- Step 16 Once the client setup is complete click Finish. See Figure B-86 and Figure B-87.

CTI OS Client - InstallShield Wizard: Cisco CTI Prod	lucts Family Release 7.5, Build 10 🔀
Select Features Select the features setup will install.	
Select the features you want to install, and deselect th CTI Toolkit Desktop Agent Desktop IPCC Supervisor Desktop Tools CTI Toolkit SDK Java Net	e features you do not want to install. Description This feature includes the CTI Toolkit Agent Desktop application.
190.85 MB of space required on the C drive 24031.74 MB of space available on the C drive InstallShield	Back Next > Cancel

CTIOS Server Information		×
	CTIOS Server A Name or IP Address: Port:	192.168.45.151 42028
	CTIOS Server B Name or IP Address: Port:	192.168.45.152 42028
	Finable Quality of Service (If you want CTIOS to have fully also enable QoS during installa NDTE: QoS does not apply to .NET CILs.	QoS) / functional QoS, you must tion of the CTIOS Server. applications using Java or
Help	< Back N	ext > Cancel

Figure B-87

If all configurations are good and communication to the CUCM via PG is active, then agent should be able to login. At this point, it is also good idea to check if calls are being routed to the agent by making a simple ICM routing script. **Start >LAA >Skill Group Selection >Stop**.

CUICM Routing Script

Create and schedule a routing script on AW by using the Script Editor software. Figure B-88 shows a sample routing script. The logic that is followed for creating this script is as follows:

Step 1	Start the script with the start node.
Step 2	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).
Step 3	Set the value of language in Call.user.microapp.locale as en-us.
Step 4	Set the value of input type (which is digits in this sample script) in <i>Call.user.microapp.input_type</i> variable to D .
Step 5	Set the value of the <i>Call.user.microapp.app_media_lib</i> to Custom .
Step 6	After setting the variables send the call to IVR using "Send to VRU" node.
Step 7	Run external script called "get4digits" that will ask the customer to enter 4 digits (i.e., an account number).
Step 8	Use the Set Variable to save the value Call.CallerEnteredDigits in the <i>Call.user.microapp.play_data</i> variable.
Step 9	Run another external scrip called <i>playdigits</i> . This script will play the value stored in <i>Call.user.microapp.play_data</i> variable.
Step 10	The select Longest Available Agent (LAA) decision object.
Step 11	If agent is available, send the caller to agent using the Skill Group node.
Step 12	If agent is not available, send the caller to Queue.
Step 13	While the caller is in queue, play agent busy and music on hold .wav files in loop.



Cisco Voice Portal Installation

Prerequisites

- The CVP server hostname should not contain any hyphen.
- Arrange for CVP license.
- Regional and language options should be set to English.

See Figure B-89.

R	tegional and Language Options	×	
	Regional Options Languages Advanced		
	Standards and formats	L	
	This option affects how some programs format numbers, currencies, dates, and time.		
	Select an item to match its preferences, or click Customize to choose your own formats:		8
	English (United States)		284 284
			CV -

Text services and input languages options should be set to English (United States) - US. See Figure B-90.

Figure B-90

Text Services and Input Languages	<u>?</u> ×	1
Settings Advanced		
Default input language Select one of the installed input languages to use when you start you computer.	r	10
English (United States) - US	•	22816

Only one Ethernet connection should be active on the machine. See Figure B-91.

Figure B-91



CVP Call Server, Operation Console and Media Server Installation

In this solution deployment lab validation, CVP Call Server and the Operation Console collocated on the same machine for ease of testing.

Install the CVP server by running the **Setup.exe** program from the installation DVD. Step through the installation using the following information:

Step 1 Select Core Software, Remote Operations and System Media Files. See Figure B-92.

B-92



Step 2 Enter appropriate security certificate information. See Figure B-93.

K.509 Certificate Enter the information that you v	would like to be included in the certificate:	:
	Common Name:	CVP7
	Organization or Company Name:	Cisco
ahaha cisco	Organizational Unit or Department:	Enterprise Voice System Architect
	Locality or City:	San Jose
Unified Customer Voice	State or Province:	CA
Portal	Country Name (2 letter code):	US
	Email address:	syali@cisco.com

Step 3 Enable the Call server and the Operations console. See Figure B-94.

Figure B-94



Step 4 Enter the preshare key to use between servers and node agents software. See Figure B-95.



CVP Component Configuration

There are several components that needs to be configured before CVP can operate properly. They are as follows:

- CVP Media Server Configuration
- CVP Call Server Configuration

CVP Media Server Configuration

This setup used Microsoft IIS as the web server to host the media files. See Figure B-96.

🐌 Internet Information Services (IIS) Manager			
General End of the section Main Mark Mar			
Internet Information Services Web Service Extensions	-		
Application Pools	A Web Service Extension	Status	
± — j Web Sites	🍸 All Unknown CGI Extensions	Prohibited	
Allow	🍸 All Unknown ISAPI Extensions	Prohibited	
Duchikik	😼 Active Server Pages	Allowed	
Prohibit	🔊 Internet Data Connector	Prohibited	
Properties	🔊 Server Side Includes	Prohibited	~
	😼 WebDAV	Allowed	16
1			226

Step 1 Enable read permission to the directory where **.wav** files are saved. See Figure B-97.

Figure B-97

Directory D	iecurity	HTTP Headers	Custom Errors	ASP.NET
Web Site	Performa	ance ISAPI Filters	Home Directory	Documents
The conter	nt for this re C	source should come from: A <u>di</u> rectory located on this A <u>s</u> hare located on anothe A redirection to a <u>U</u> RL	computer er computer	
Lo <u>c</u> al path:	c	\inetpub\wwwroot	В	r <u>o</u> wse
I Script so I Read I Write I Director	ource acces: y <u>b</u> rowsing	s I♥ Log ▼ Ind	ex this resource	
Application	settings			
Application Application	settings na <u>m</u> e:	Default Application		R <u>e</u> move
Application Application (Starting poi Execute per	settings na <u>m</u> e: nt: rmissions:	Default Application <default site="" web=""> Scripts only</default>		Remove
Application Application Starting poi Execute per Application	settings na <u>m</u> e: nt: rmissions: pool:	Default Application <default site="" web=""> Scripts only DefaultAppPool</default>	Conl	Remove Figuration

Step 2 Either create a Virtual Directory linking to the Media Files installed by the CVP **setup.exe**, or copy the "**en-us**" folder to the root of the IIS Web server. See Figure B-98.
rigure D-90	Fiaure	B-98
-------------	--------	------

Virtual Directory Documents Directory Security				
The content for this reso	urce should come from:			
• A	directory located on this computer			
C A :	share located on another computer			
C Ar	redirection to a <u>U</u> RL			
Local path: C:\I	MediaFiles\en-us	Browse		
Script source access ✓ Log visits Read ✓ Index this resource Write ✓ Directory browsing				
Application settings				
Application name:	en-us	Remove		
Starting point:	<default site="" web="">\en-u</default>			
Execute permissions:	Scripts only			
Application pool: DefaultAppPool 🔽 Unload				

Step 3 Make sure anonymous access is enabled and the built-in IIS User is assigned. See Figure B-99.

Figure B-99

Use the followi	ing Windows user account for anonymous access:
<u>U</u> ser name:	IUSR_MEDIA Browse
Password:	•••••
Authenticated - For the followin	access
are required wi	hen:
	inorm in the second
- anon - acces	ivmous access is disabled, or ss is restricted using NTFS access control lists
- anon - acces Integrated	wmous access is disabled, or ss is restricted using NTFS access control lists Windows authentication
- anon - acces Integrated Digest auth	wmous access is disabled, or ss is restricted using NTFS access control lists Windows authentication nentication for Windows domain servers
- anon - acces Integrated Digest auth Basic authe	wmous access is disabled, or ss is restricted using NTFS access control lists Windows authentication nentication for Windows domain servers entication (password is sent in clear text)
- anon - acces Integrated Digest auth Ba <u>s</u> ic authe .NET Passp	www.saccess is disabled, or ss is restricted using NTFS access control lists Windows authentication nentication for Windows domain servers entication (password is sent in clear text) oort authentication
- anon - acces Integrated Digest auth Basic authe .NET Passp	wimous access is disabled, or ss is restricted using NTFS access control lists Windows authentication nentication for Windows domain servers entication (password is sent in clear text) bort authentication
- anon - acces Integrated Digest auth Basic authe .NET Passp Default dome	winous access is disabled, or ss is restricted using NTFS access control lists Windows authentication hentication for Windows domain servers entication (password is sent in clear text) bort authentication ain:

Step 4 Create a folder named **Custom** below the **en-us** folder for the audio files in the custom scripts. See Figure B-100.



CVP Call Server Configuration

Before configuring CVP call server, it should be important to know little bit about the setup and SIP call flows. Notices that these call flows are valid for the Type 10 VRU only. Also notice that "**cid**" is actually the correlation ID and is a numerical value.

Call Flow

CUCM Originated Calls

Table B-3 CUCM Originated Calls

CUCCE Pilot Number	IP Phone caller dials CTI route point number 1000	
Routing Client	SIP Gateway is the routing client	
Label Returned to SIP GW by CUICM	1000+cid	
Processing at SIP GW	SIP GW receives the label and sends the call to CVP Call Server	
Processing at CVP	CVP receives this label and send it to CUICM as a new route-request.	
Routing Client	Notice that now CVP is the routing-client	
Processing at CUICM	CUICM receives its own generated label again and knows that loop is complete. And then generates a new label 1000+cid and sends to CVP	

Processing at CVP	CVP Call Server send this label 1000+cid to VXML-GW	
Processing at VXML-GW	VXML-GW has an incoming dial-peer configured that basically invokes the bootstrap tcl service	
	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 1000+cid to CUICM to inform that VXML-GW resources are engaged	

Table B-3 CUCM Originated Calls (continued)

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. Using the SIP Gateway, a single static route can be used, (e.g., >, sip-1.cisco-irn.com)

CVP Operation Console Server

CVP Operation Console Server provides web-based front-end to configure different components in CVP environment.See Figure B-101 and Figure B-102.

Figure B-101 CVP Call Server General Setting

General ICM SIP IVR Device Pool Infrastructure				
General		Activate Services		
IP Address: *	192.168.45.131	ICM: 🔽		
Hostname: *	cvp-1.cisco-irn.com	IVR: 🔽		
Description:		SIP: 🔽		
Enable secure communication with the Ops console:	1	H.323: Change Type		
		J *		

Figure B-102

neral	Pool Statistics					
						Refresh: No Refresh 💽 Go
evid	es					
_	Hostname	IP Address	Device Type	Actions	Status	Active Calls
0	cvp-1.cisco-irn.com	192.168.45.131	Call Server	3	Up	0
5	icm-a.cisco-irn.com	192.168.45.141	ICM Server		N/A	N/A
)	icm-b.cisco-irn.com	192.168.45.142	ICM Server		N/A	N/A
5	sip-1.cico-irn.com	192.168.45.188	SIP Proxy Server	2 2	N/A	N/A
						Page 1 of 1
					Edit Start Shu	tdown Graceful Shutdown
e:E	ach column can be sorte	d by clicking the colu	mn header. This sorting is on	a per-page basis only.		

CVP Call Server ICM Configuration

See Figure B-103.

General ICM SIP IVR Device Pool Infrastructure	
General Configuration VRU Connection Port: * 5000 Maximum Length of DNIS: * I0 DNIS C Add: Add DNIS Delete DNIS I Add DNIS	Advanced Configuration New Call Service ID: * Pre-routed Call Service ID: * New Call Trunk Group ID: * Pre-routed Call Trunk Group ID: * Pre-routed Call Trunk Group ID: * Select QoS level: Ccs3 1

CVP Call Server SIP Configuration and Static Route

Default information was used and no fields were modified. See Figure B-104.

Figure B-104

General ICM SIP IVR Device Pool Infra	astructure		
Configuration		Local Static Routes	
Enable outbound proxy:	C _{Yes} 🖲 No 1	Static routes for local routing without an outbound proxy -	
Use DNS SRV type query:	C Yes 🖲 No 1	Dialed Number (DN):	
Resolve SRV records locally:	□ 1	IP Address/Hostname:	
Outbound proxy Host:	- 🔽 1	Add Remove	
Outbound SRV domain name (FQDN):	1	>,sip-1.cisco-irn.com Move Up	
Outbound proxy Port:	5060	Move Down	
Outgoing transport type:	UDP • 1		
Port number for incoming SIP requests: *	5060 1	Dialed Number (DN) patterns	
Incoming transport type:	TCP+UDP 💽 1	Patterns for sending calls to the originator -	
DN on the Gateway to play the ringtone: *	91919191	Add Berrova	
DN on the Gateway to play the error tone: *	92929292		
Time to wait for ICM instructions: *	2000 milliseconds		75
SIP info tone duration: *	100 milliseconds	Patterns for RNA timeout on outbound SIP calls -	90B4

VXML and Ingress Gateway Configuration

In this setup, the same router can be used as an ingress gateway as well as the VXML gateway. Note that due to VXML compatibility issues, all Cisco IOS versions are not supported. In this lab validation tested **c2800nm-ipvoicek9-mz.124-24.T1.bin**.

Copy following files to VXML Gateway router's flash memory:

```
bootstrap.tcl
bootstrap.vxml
cvperror.tcl
CVPSelfService.tcl
CVPSelfServiceBootstrap.vxml
survivability.tcl
handoff.tcl
ringtone.tcl
recovery.vxml
```

holdmusic.wav

```
ringback.wav
pleasewait.wav
critical_error.wav
en_0.wav
en_1.wav
```

Configuration

```
version 12.4
service timestamps debug datetime localtime show-timezone
service timestamps log datetime localtime show-timezone
no service password-encryption
1
hostname VXML
1
boot-start-marker
boot system flash c2800nm-ipvoicek9-mz.124-24.T1.bin
boot-end-marker
1
logging message-counter syslog
logging buffered 100000
enable password cisco
1
no aaa new-model
clock timezone PST -8
clock summer-time PSTDST recurring
dot11 syslog
ip source-route
1
1
ip cef
1
1
ip domain name cisco-irn.com
ip name-server 192.168.42.130
no ipv6 cef
ntp server 192.168.0.1
ntp server 192.168.42.130
ntp server 192.168.62.161 prefer
ntp server 192.168.62.162
multilink bundle-name authenticated
!
!
voice service voip
allow-connections h323 to h323
allow-connections h323 to sip
allow-connections sip to h323
 allow-connections sip to sip
 fax protocol cisco
h323
 emptycapability
 no telephony-service ccm-compatible
  no ccm-compatible
 h225 id-passthru
  call start slow
 h245 passthru tcsnonstd-passthru
 sip
  ds0-num
```

```
header-passing
!
I.
I.
voice class codec 1
codec preference 1 g711ulaw
codec preference 2 g729r8
!
voice class h323 1
 h225 timeout setup 3
!
Т
voice translation-rule 1
rule 1 /987654/ //
I.
Т
voice translation-profile block
translate called 1
!
!
voice-card 0
dsp services dspfarm
1
http client cache memory pool 15000
http client cache memory file 500
ivr prompt memory 15000
1
application
 service new-call flash:bootstrap.vxml
 paramspace english language en
 paramspace english index 0
 paramspace english location flash:
 paramspace english prefix en
 1
 service cvp-survivability flash:survivability.tcl
 paramspace english language en
 paramspace english index 0
 param alert-timeout 20
  paramspace english location flash
 paramspace callfeature med-inact-det enable
 param setup-timeout 7
 paramspace english prefix en
 1
 service ringtone flash:ringtone.tcl
 paramspace english language en
 paramspace english index 0
 paramspace english location flash
 paramspace english prefix en
 1
 service recovery flash:recovery.vxml
 paramspace english language en
 paramspace english index 0
 paramspace english location flash:
 paramspace english prefix en
 1
 service cvperror flash:cvperror.tcl
  paramspace english index 0
  paramspace english language en
  paramspace english location flash
 paramspace english prefix en
 1
 service takeback flash:survivability.tcl
  paramspace english language en
  paramspace english index 0
```

paramspace english location flash

```
paramspace english prefix en
 Т
 service HelloWorld flash:CVPSelfService.tcl
 paramspace english index 0
 paramspace english language en
 param CVPSelfService-port 7000
  param CVPSelfService-app HelloWorld
  param CVPPrimaryVXMLServer 192.168.45.131
  paramspace english location flash
  paramspace english prefix en
 param CVPBackupVXMLServer 192.168.45.132
 1
 service handoff flash:handoff.tcl
 paramspace english language en
 paramspace english index 0
 paramspace english location flash
 paramspace english prefix en
 service bootstrap flash:bootstrap.tcl
  paramspace english index 0
 paramspace english language en
 paramspace english location flash:
 paramspace english prefix en
 T
!
vxml version 2.0
1
archive
log config
 hidekeys
!
!
interface FastEthernet0/0
description Connection to SACCESS-g1/33
 ip address 192.168.45.101 255.255.255.0
duplex auto
 speed auto
I
interface FastEthernet0/1
no ip address
shutdown
 duplex auto
 speed auto
1
interface GigabitEthernet1/0
no ip address
shutdown
1
1
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.45.1
!
ip http server
no ip http secure-server
1
control-plane
mgcp fax t38 ecm
mgcp behavior g729-variants static-pt
1
! <====Configuration for Trusted Relay===>
sccp local FastEthernet0/0
sccp ccm 192.168.45.182 identifier 1 version 7.0
```

```
sccp ccm 192.168.80.181 identifier 2 version 7.0
sccp
1
sccp ccm group 1
associate ccm 1 priority 1
associate profile 1 register MTP-01
1
sccp ccm group 2
associate ccm 2 priority 1
associate profile 2 register MTP-02
!
dspfarm profile 2 mtp
codec g711ulaw
codec pass-through
maximum sessions software 110
associate application SCCP
1
dspfarm profile 1 mtp
codec g711ulaw
 codec pass-through
maximum sessions software 110
associate application SCCP
! <===End Configuration for Trusted Relay===>
!
dial-peer voice 9191 voip
service ringtone
 session protocol sipv2
 incoming called-number 9191T
 dtmf-relay rtp-nte
codec g711ulaw
no vađ
!
dial-peer voice 9292 voip
service cvperror
session protocol sipv2
incoming called-number 9292T
dtmf-relay rtp-nte
codec g711ulaw
no vad
1
dial-peer voice 1006 voip
translation-profile incoming block
service bootstrap
session protocol sipv2
incoming called-number 1006T
dtmf-relay rtp-nte
codec g711ulaw
 ip qos dscp cs3 signaling
no vad
1
dial-peer voice 987654 voip
translation-profile incoming block
incoming called-number 987654
1
1
1
line con 0
exec-timeout 0 0
line vty 0 4
exec-timeout 0 0
password cisco
login
line vty 5 15
 exec-timeout 0 0
```

```
password cisco
login
!
scheduler allocate 20000 1000
end
```

Expert Advisor Installation

The installation is on VOS. It is very simple. Refer to the *Installation Guide for Cisco Unified Expert* Advisor 7.6(1) for additional information. Follow these steps:

- Step 1 Media Check: select Yes if you want to check the media.
- Step 2 Product Deployment Selection: Click OK.
- Step 3 Proceed with Install: Yes.
- Step 4 Platform Installation Wizard: Click on Proceed.
- Step 5 Apply Patch: Click No.
- Step 6 Basic Install: Click on Continue.
- **Step 7** Timezone Configuration: Select your timezone.
- **Step 8** Auto Negotiation Configuration: Select the default option **Yes**.
- **Step 9** MTU Configuration: Select the default option: No.
- Step 10 DHCP Configuration: Select No.
- **Step 11** Static Network Configuration: Enter the information for your network.
- Step 12 DNS Client Configuration: Click Yes.
- **Step 13** DNS Client Configuration: Enter your DNS information.
- **Step 14** Administrator Login Configuration: Enter your Administrator ID and password information.
- Step 15 Certification Information: Enter your Certificate Information.
- Step 16 First Node Configuration: Click Yes if you are installing your first node. If you are installing the second Expert Advisor Server or the reporting server, click No.
- Step 17 Network Time Protocol Client Configuration: Click Yes.
- **Step 18** Network Time Protocol Client Configuration: Enter the NTP Client information.
- **Step 19** Database Access Security Configuration: Enter the system security password.
- **Step 20** SMTP Host Configuration: Select **No** if you are not configuring a SMTP Host for this machine.
- **Step 21** Application User Configuration: Enter the Application (GUI) username and password.
- Step 22 Platform Configuration Confirmation: Click on Ok.
 For more information on the installation of the Expert Advisor servers, refer to the *Installation Guide* for Cisco Unified Expert Advisor 7.6(1).

CUP Installation

The CUP installation is very similar to the installation of Expert Advisor, since it is also running on Unified Communications Operating System (UCOS). Follow the steps above for base installation.

Once the server is installed, a few post install steps need to be done; log into the server via the web interface: http://<YourCUPServerAddress>/ccmadmin.

After the install, enter the post install information. See Figure B-105 to Figure B-109.

Figure B-105

11	Post-Installation Deployment Wizard
	The final install steps for this Cisco Unified Presence server need to be completed. The following screens will walk you through this process.
	The Cisco Unified Communications Manager Publisher is the node that the CUP server will communicate with to receive end user updates.
	Cisco Unified Communications Manager Publisher configuration:
TP	Hostname* cm-2
0-1-0	IP Address 192.168.45.182
0	- Back Next

1200	Post-Installation	Deployment Wizard
AXL is the API that CUP uses to communicate with the CUCM Publisher. Com via AXL requires AXL login information from the CUCM Publisher.		
	AXL Configuration Inform	ation:
	CUCM Publisher IP Address	192.168.45.182
	AXL User*	CUPsecureuser
	AXL Password*	•••••
0-1-0	Confirm Password*	•••••
0	Back Next	

Figure B-107

1 2 2 2 2	Post-Installation Deployment Wizard The IPSec Security password is used to secure communication among CUCM and CUP nodes. This password must match the security password as configured on the CUCM Publisher node.		
1.115.2	Security Password	configuration:	
	Security Password*	•••••	
P	Confirm Password*	•••••	
0-1-0			
0	- Back Next -		





Post-Installation D	eployment Wizard
Post-Installation Deployment has next.	been completed. Click below where you want to go
Home	- Administration Home Page
System Dashboard	- System Dashboard
Topology	- System Topology

Obtain a license. Upload the license. See Figure B-110.

Fi	gure l	B- <i>110</i>			
Sys	tem 👻	Presence 👻	Application 👻	User Management 👻 Bulk Administration 👻	
	Cluster	Topology			
	CUCM	Publisher			
	Applica	ation Listeners			
	Licensi	ing	•	License File Upload	
	Securit	У	•	License Unit Report	5
	Service	e Parameters			228

Configuration

CUP

Step 1 Activate the Cisco UP SIP Proxy, Cisco UP Presence and Cisco UP Sync Agent Services. See Figure B-111.

Figure B-111

Serve	rr* sip-1.cisco-irn.com ▼ Go	
🗆 ci	heck All Services	
Data	base and Admin Services	
	Service Name	Activation Status
\checkmark	Cisco AXL Web Service	Activated
◄	Cisco Bulk Provisioning Service	Activated
Perfo	irmance and Monitoring Services	
	Service Name	Activation Status
~	Cisco Serviceability Reporter	Activated
CUP	Services	
	Service Name	Activation Status
•	Cisco UP SIP Proxy	Activated
V	Cisco UP Presence Engine	Activated
	Cines UD Curs Annut	Activated

Step 2 Go to **Presence > Routing > Static Routes**. See Figure B-112.

Figure B-112

cisco	(F	C isco (Unified Pr	esenco unications	e A sol	Administration			
System 👻	Pre	sence 👻	Application -	User Man	agen	nent 👻 Bulk Administration 👻	Diag	nostics 👻	Help 🖣
		Settings	4						
		Inter-Clu	stering						
		Inter-Dor	nain Federation						
Cisc		User-Age	ent Configuration		10	Iministration		n i	
System		Routing		•		Settings			
System		131011.7	.0.4.10000-1	0		Static Routes			
						Method/Event Routing			
						Number Expansion			

- Step 3 And add routes to the Expert Advisor Runtime server. See Figure B-113.

Figure	B-	113
riguic	-	

Stat	Static Route (1 - 7 of 7) Rows per Page 50 •								
Find :	ind Static Route where Destination Pattern 🔻 begins with 💌 🛛 🗐 🖉 🚍								
	Destination Pattern *	Blocked	Description	Next Hop	Next Hop Port	Priority	Weight	Protocol Type	In Service
	<u>1005*</u>		To send the call to CVP	cvp-1.cisco-irn.com	5060	1	1	UDP	On
	1006*		To send the call to the VXML GW	vxml.cisco-irn.com	5060	1	1	UDP	On
	<u>12</u>		Translation Routes to Expert Advisor	ea-1.cisco-irn.com	5060	1	1	UDP	On
	5		To branch phones	cm-2.cisco-irn.com	5060	1	1	UDP	On
	<u>6</u>		To branch phones	cm-2.cisco-irn.com	5060	1	1	UDP	On
	<u>91919191</u>		Ring tone	vxml.cisco-irn.com	5060	1	1	UDP	On
	92929292		Error Tone	vxml.cisco-irn.com	5060	1	1	UDP	On
Add	New Select All	lear All	Delete Selected						

Create a Presence Gateway so that Unified CM can send presence information to the Cisco Unified Step 4 Presence Server. Go to Presence > Presence Gateways. See Figure B-114.

You can configure a Cisco Un then send SIP Subscribe mes Presence server to receive pu	i ettings (Cisco Unified Communications Manager) ified Communications Manager server as a presence gateway. The Cisco Unified Presence server will sages to Cisco Unified Communications Manager over a SIP trunk which will allow the Cisco Unified resence information (e.g. phone on/off hook status).
Presence Gateway Type*	CUCM
Description*	cm-2 SIP gateway
Presence Gateway*	cm-2.cisco-irn.com
— Save Delete Add New	·

- Step 5 Configure a Proxy Domain so that CUPC users can connect to the CUP server to obtain presence information. Go to System > Service Parameters.
- Step 6 Set the "Proxy Domain" field to the correct DNS domain.
- Step 7 Configure Incoming ACL: configure which hosts, domains, and CUPC clients can access CUP Server.
- Go to System > Security > Incoming ACL. See Figure B-115. Step 8

Incoming	ACL Entry (1 - 8 of 8)		Rows per Page 50 💌
Find Incomi	ng ACL Entry where Address Pattern 💌 be	gins with 💌 Find 🔹	Clear Filter 🛛 🔂 📼
	Address Pattern 🕈	Description	
	10.10.	all store hosts	
	192.168.	all hosts in 192.168.x.x	
	<u>192.168.81.101</u>	Expert Advisor - ea-1.cisco-irn.com	
	cm-2.cisco-irn.com	System Generated Allow Rule	
	cvp-1.cisco-irn.com	CVP Server	
	cvp-2.cisco-irn.com	CVP Server	
	sip-1.cisco-irn.com	System Generated Allow Rule	
	vxml.cisco-irn.com	calls to v×ml gateway	
Add New	Select All Clear All Delete Selec	ted	

Step 9 Configure TFTP Server for CUPC.

Step 10 Go to **Application > Cisco Unified Personal Communicator > Settings**. See Figure B-116.

Figure B-116

— 🛃 CUPC Global S	ettings	
Proxy Listener*	Default Cisco SIP Proxy TCP Listener	
Primary TFTP Server	cm-2.cisco-irn.com	
Backup TFTP Server		
Backup TFTP Server		8187
		N.

- **Step 11** Add SIP Publish capability to the SIP trunk between CUCM and CUP. This will allow CUCM to provide phone presence information to CUP server.
- **Step 12** Go to the CUP server, **Application > Presence > Settings**.
- Step 13 Check the Enable SIP Publish on CUCM.
- **Step 14** Select the SIP trunk configured on CUCM. See Figure B-117.

—🗾 Global Setting	s	٦				
CVP Enable ACL Configuration						
🗹 Enable Instant Me	ssaging (cluster-wide)					
🗹 Enable/Disable ab	lity for users to view presence on blocked users					
🗖 Enable Email ID fo	r Federation					
Max Contact List Size (per user)* Max List Box Items* Cluster ID*	200 250 StandAloneCluster					
🖵 🗹 Enable SIP Pu	blish on CUCM					
CUCM SIP Publish Trunk	SIP-1_Proxy	28188				
		ЦŇ				



Another way to do this is to go directly to the CUCM admin page, Service Parameter, Cisco CallManager, and select the SIP trunk in the field CUP Publish Trunk

Step 15 Configure Conferencing hosts as appropriate. Go to Application > Cisco Unified Personal Communicator > Conferencing Server>New servers. See Figure B-118.

Figure B-118

Confe	rencing Host (1 - 2 of 2)				Rows per Page 50 💌
Find Co	nferencing Host where Name	💌 begins wi	th 🔽 Find	Clear Filter	4 -
	Name 🕈	Description	Hostname/IP Address	Port	Server Type
	Meeting Place Express	MPX 211	mp3.cisco-irn.com	80	MeetingPlace Express
	VEM Webex Conference	lab webex	ciscocmo-dev.webex.com	443	WebEx
Add N	New Select All Clear All	Delete Selected			

Step 16 After the server is configured, create a Conferencing profile and add users to the profile. See Figure B-119.

Name	•	VEM users Desktop Share			
Descri	ption	VEM collaborative desktop	sharing		
Primar	y Conferencing Server*	Meeting Place Express		•	
Backu	o Conferencing Server	< None >	•		
Backu	o Conferencing Server	< None >		•	
🗹 Ma	ke this the default Conferen	cing Profile for the system.			
- 🎒 ւ	Jsers in Profile				
	User ID	First	name	Lastname	
	<u>Jack3</u>	jack3		Large	
d Pro	visioning Guide				
	jack2	Jack		Large	
	<u>iill1</u>	Jill		Small	
	<u>iill2</u>	Jill		Small	
	<u>iill3</u>	jill3		Small	
	<u>iohn1</u>	john		mini	
	john2	John		Mini	
	<u>john3</u>	john3		mini	
	Add Users to Profile	Select All Clear All	Delete Selected	Rows per Page	

CUCM

Since in this solution calls are originated from an IP Phone, create a CTI RP (you could also send the call to CVP with a Route Pattern, but here, the scenario covers where the call is sent to CVP using a CTI RP) and add a DN for this CTI RP(in our example, 1000 and 1301 DNs are used). If your calls are coming directly to CVP via a PSTN GW, you do not need these steps. See Figure B-120 and Figure B-121.

Figure B-120

—Device Information ———		
Registration	Registered with Cisco Unified Communications Manager	cm-2.cisco-irn.com
IP Address	192.168.45.152	
Device Name*	CTI-RP-1000	
Description	CTI-RP Cti Route Point 1000	
Device Pool*	Default	<u>View Details</u>
Common Device Configuration	< None >	View Details
Calling Search Space	< None >	
Location *	Hub_None	
User Locale	< None >	
Media Resource Group List	< None >	
Network Hold MOH Audio Source	< None >	
User Hold MOH Audio Source	< None >	
Use Trusted Relay Point*	Default	
Calling Party Transformation CSS	< None >	
Geo Location	< None >	
🗹 Use Device Pool Calling Party	Transformation CSS	
Association Information		
•77: Line [1] - 1000 (no partition)		
erns		
<u>errs Line 2 - Add a new DN</u>		

Save Delete

Copy Reset

Apply Config Add New

Figure B-121

СТІ	CTI Route Point (1 - 2 of 2) Rows per Page 50 💌								
Find	Find CTI Route where Device Name 💌 begins with 💌 Find Clear Filter 🕂 📼 Select item or enter search text 💌								
	Device Name [▲]	Description	Device Pool	Calling Search Space	Partition	Extension	Status	IP Address	Сору
	<u>CTI-RP-</u> 1000	CTI-RP Cti Route Point 1000	<u>Default</u>			<u>1000</u>	Registered with cm-2.cisco- irn.com	192.168.45.152	ß
	<u>CTI-RP-</u> <u>1301</u>	Route for Expert Advisor	<u>Default</u>			<u>1301</u>	Registered with cm-2.cisco- irn.com	192.168.45.152	6
Ad	ld New	Select All Clea	r All 📃 I	Delete Selecte	ed R	eset Selecte	d Apply C	onfig to Selected	

Step 1 Associate the CTI-RP to the jtapi user that the Agent PG is using to connect to CUCM. See Figure B-122.

228191

Figure B-122

Application User Information	
User ID* jtapi	Edit Credential
Password	••
Confirm Password	••
Digest Credentials	
Confirm Digest Credentials	
Presence Group * Standard Presence group	×
C Accept Presence Subscription	
C Accept Out-of-dialog REFER	
Accept Unsolicited Notification	
C Accept Replaces Header	
- Device Information	
Available Devices	Find more Phones
	Find more Route Points
	Find more Pilot Points
×	
Controlled Devices CTI-RP-1000	
SEP0017956DD439	
SEP001/E0355BCD SEP0018199456D4	338 ¹

Step 2 Add the CUP server in the Application server Configuration as shown in Figure B-123 and Figure B-124.

Sys	tem 👻	Call Routing 👻	Media Resour	
	Server			
	Cisco L	Inified CM		
	Cisco L	Inified CM Group		
	Phone I	NTP Reference		
	Date/Tir	ne Group		
	Presen	ce Group		
	Region			
	Device	Pool		
	Device	Mobility	•	
	DHCP		•	
	LDAP		•	
	Locatio	n		
	Physica	al Location		
	SRST			
	MLPP		•	
	Enterpr	ise Parameters		
	Enterpr	ise Phone Configu	ration	
	Service	e Parameters		
	Securit	y Profile	•	5
	Applica	tion Server	A Pool	2222

Figure B-124

Application Server Application Server	er Information Type Cisco Unified Presence Server	
Name*	SIP-1.cisco-irn.com	
URL		
End User URL		
— Save Delete	Copy Add New	228195

Step 3 If the expert advisor user will use CUPC as a softclient, create a phone device on CUCM for the CUPC softclients. Select the **Cisco Unified Personal Communicator** Phone Type. See Figure B-125.

Figure B-125

—Select the ty	pe of phone you would like to create—		ဖ္တ
Phone Type*	Cisco Unified Personal Communicator	•	281

Step 4 The device name must start with UPC and be followed, all capital letters, by the username of the expert advisor that will use the client. See Figure B-126.

Figure B-126

– Phone Type Product Type: Cisco Unified Personal Communicator Device Protocol: SIP						
Device Information			_			
Registration	Unknown					
IP Address	Unknown					
🗹 Is Active						
Device Name*	UPCJOHN1					
Description	John 1 Mini					
Device Pool*	Default	View Details				
Common Device Configuration	< None >	View Details				
Phone Button Template*	Standard Unified Communicator SIP	•	01			
Common Phone Profile*	Standard Common Phone Profile	-	100			

Step 5 Add a DN for each of the CUPC device.

Step 6 Add expert advisor users as shown in Figure B-127.

System 👻 Call Routing	✓ Media Resources Voice Mail Device Applica	ation 👻	User Management 👻 Bulk Administration 👻
End User Configurat	ion		Credential Policy Default
			Credential Policy
Save 🗙 Delete	Add New		Application User
			End User
- Status			Role
Status: Ready			User Group
			User/Phone Add
 User Information — User ID* 	iaha1		Application User CAPE Profile
Password		Н	End User CAPE Profile
Confirm Password		4	SID Basic
DIN		_	Sir Realm
Confirm DIN	•••••		Edit Credential
Confirm PIN	•••••		
Last name	mini		
Middle name	1		
First name	john		
Telephone Number			
Mail ID			
Manager User ID			
Department	1passw0rd!		
User Locale	< None >	-	
Associated PC			
Digest Credentials			
Confirm Digest Creden	ntials		
Device Associations			_
Controlled Devices SE	P00258418216A		
0F	-001111		Device Association
1			

Step 7 In the *Directory Number Association* field, select the primary Extension for the user. See Figure B-128.

Directory Numbe	Associations —	
Primary Extension	6002	₹ X
		5

Step 8 If allowing CTI deskphone mode for the users, make the user part of the Standard CTI Enabled user group. See Figure B-129.

Figure B-129

Groups	Standard CCM End Users Standard CTI Enabled	Add to User Group
		View Details
Roles	Standard CCM End Users Standard CCMUSER Administration Standard CTI Enabled	
		View Details

Step 9 For each Expert Advisor user, go to their phone configuration and then line configuration, go to the section Users Associated with Line, and associate the end user (expert advisor user) that will use this phone. See Figure B-130.

Figure B-130

- User	s Associated with Line		
	Full Name	User ID	Permission
	<u>mini, john</u>	john1	١
	Associate End Users	Select All Clear All	Delete Selected

This will change the CUPC client availability to "On the Phone" when the expert advisor user goes off hook on one of his associated phone devices.

Step 10 Add an CUCM user for each Expert Advisor Runtime server. See Figure B-131.

User Information ——			
User ID*	ExpertAdvisorSystem		
Password	•••••	Edit Credential	
Confirm Password	•••••		
PIN	•••••	Edit Credential	
Confirm PIN	•••••		
Last name *	System		
Middle name	Advisor		2
First name	Expert		acc

- **Step 11** Enable presence and CUPC capabilities for the Expert Advisor users and also for the user that the Expert Advisor runtime server will use to connect to CUP (in our case, ExpertAdvisor user).
- Step 12 In System > Licensing > Capabilities Assignment, enable CUP and CUPC for each Expert Advisor user. See Figure B-132.

Figure B-131



Step 13 Configure a SIP Trunk between CUCM and CUP server (enter the IP address or DNS name of the CUP server in the *Destination Address* field). See Figure B-133.

Figure B-133

		Name *	Description	Calling Search Space	Device Pool	Route Pattern	Partition	Route Group	Priority	Trunk Type	SIP Trunk Security Profile	
	8	SIP-1 Proxy	Trunk to CUP Server		Default	1005!				SIP Trunk	Non Secure SIP Trunk Profile	
	ë	nice-1	SIP Trunk to NICE Server		Default			Route-to-NICE-1	1	SIP Trunk	Non Secure SIP Trunk Profile	33
Ad	d New	Select All	Clear All Delete Selected	Reset Selected	Apply	Config to Select	ed					0080

CUP Server Configuration

LDAP Configuration

LDAP is an optional component of the Unified Expert Advisor system and is not required for routing requests. It allows Expert Advisor users to search through the AD with their CUPC client.

Step 1 Go to **Application > Cisco Unified Personal Communicator > LDAP Server**. See Figure B-134.

Figure B-134

LDAP Host Config	juration —	
Name*	Cisco-IRN LDAP	
Description	Activedirectory server	
Hostname/IP Address*	activedirectory.cisco-irn.com]
Port*	389	
Protocol Type*	ТСР	ĺ

Step 2 Go to: Application > Cisco Unified Personal Communicator > LDAP Profile.

Step 3 Enter the information of your LDAP directory and click on **Add Users to profile**. The users that are shown are the users entered in CUCM that were downloaded into CUP server, with the right capability settings configured in CUCM administration page. See Figure B-135.

г١	🔉 LDAP Profile Configura	tion		
N	ame*	Cisco-irn LDAP_Profile		
D	escription	ActiveDirectory Profile		
в	ind Distinguished Name (DN)	administrator@cisco-irn.com	🗖 Anonymous Bind	
P	assword			
С	onfirm Password			
s	earch Context	cn=users, dc=cisco-irn, dc=com	🗷 Recursive Search	
P	rimary LDAP Server*	Cisco-IRN LDAP		
В	ackup LDAP Server	< None >		
В	ackup LDAP Server	< None >		2d
F	Make this the default LDAP F	Profile for the system.		22822

- Step 4 If you are deploying OCS/LCS and want to enable deskphone control with CUPC, go to Application > Deskphone Control > Settings.
- Step 5 Select On for the Application Status and enter the jtapi CtiGw information and CTIM information. See Figure B-136.

Figure B	-136
----------	------

Control Se	ettings	
The Deskphone control applicat clients that provide Click-to-Dia to a maximum of eight CUCM s	ion provides connectivity between Cisco Unified Commu I/Phone control-type services. You can configure the De: ervers.	nications Manager (CUCM) and soft skphone control application to connect up
Application Status*	On 💌	
Application Username	CtiGw	
Application Password		
Confirm Password	•••••••••••••••••	
Heartbeat Interval (seconds)*	8	
Session Timer (seconds)*	1810	
Microsoft Server Type*	MOC server OCS	8
CUCM Address (1 of 8)	192.168.45.182	222

Step 6 Select Application > Deskphone Control > User Assignment and check the Enable Deskphone Control checkbox. See Figure B-137.

Figure B-137	
User ID: john1	-
■ Deskphone Control Assignment ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	-
Save	228209



You do not have to go to **Application > Deskphone Control > Settings** in order to enable **Deskphone Control**, if you are not using OCS/LCS.

Expert Advisor Configuration

Step 1 Go to http://<EA-ip-address>. Expert Advisor system can be deployed with expert advisor users using either Cisco Unified Presence or Microsoft Office Communicator, not both types in the same Expert Advisor deployment. See Figure B-138.

Figure B-138

Please select the type of IM clients your experts will be using to connect to Expert Advisor.

IMPORTANT: This setting is permanent and cannot be changed without re-installing Expert Advisor and re-entering your configuration.

Cisco Unified Presence
 C Microsoft Office Communicator

Step 2 Go through the Guided Configuration Wizard. See Figure B-139.

Figure B-139

Start Guided Configuration Wizard		
Nould you like to configure the System using the Guided Configuration Wizard?		
🗆 Do not ask again	OK Cancel	228211

Step 3 Upload the license. If not, the system comes with a default license of 5 users. See Figure B-140.

Figure B-140

Configure License	
Please browse to and upload your license file, which sets	; the number of Expert Advisors you are authorized to enable.
Current License Total Licenses available for Enabled Expert Advisors:	5
License File Management Select a local license file to upload :	C:\Documents and Settings\Administrator\Deskt(Browse

Step 4 Configure the Primary Runtime Server. In the *CUP user* field, enter the CUP user that Expert Advisor runtime server will use to connect to the CUP server. See Figure B-141.

Configure Runtime Server—		
Туре:	Primary	_
"Name:	ea-1.cisco-irn.com	
* Host Address:	192.168.81.101	
Description:		
Cisco Unified Presence Serve	er	Port pumber
* ¹ CUP server:	sip-1.cisco-irn.com	5060
* ¹ CUP server proxy domain:	cisco-irn.com	
* ¹ CUP user:	ExpertAdvisorSystem	

Step 5 Configure the secondary Runtime Server. Skip if you do not deploy a HA Runtime server. See Figure B-142.

Configure High Availability Serve	er	
⊤Configure Runtime Server		
Туре:	High Availability	
*Name:		_
* Host Address		_
Host Address:		_
Description:		
Cisco Unified Duppenso Comu		
Cisco onnieu Presence Server	Host Address	Port number
* ¹ CUP convert		5060
COP Server,		10000
*1 CUP server proxy domain:	cisco-irn.com	
* ¹ CUP user:		
*Required fields		
¹ Change in value requires device	restart	
	Back Next S	Skin Cancel Heln
	Dack Next	Concer Help

Figure B-142

228214

Step 6 Configure an Expert Advisor reporting server. Skip if you do not deploy a Expert Advisor reporting server. See Figure B-143.

Configure Reporting Server General Name: EA-2.cisco-irn.com Host Address: 192.168.81.121 Description: EA Reporting Server for VEM Reporting Properties Define the maximum disk space to use to persist reporting data on the runtime servers during reporting server outages or loss of connectivity. Max Storage Size (MB): 2048 Restore Default *Required fields			
⊂ General			
*Name:	EA-2.cisco-in	n.com	
*Host Address:	192.168.81.1	121	
Description:	EA Reporting) Server for VEM	
Reporting Properties			
Define the maximum disk space reporting server outages or loss	to use to persist repo of connectivity.	rting data on the runtime servers during	
*Max Storage Size (MB):	2048	Restore Default	
		Back Next Skip Cancel Hel	<mark>,</mark>

Step 7 Configure a AD server. See Figure B-144.

Configure Active Directory		
Active Directory Server		
*Host Address for Primary Active Directory Server:	* Port:	Use SSL:
activedirectory.cisco-irn.com	389	
Host Address for Redundant Active Directory Server:	Port:	Use SSL:
	389	
*Manager Distinguished Name:	CN=Administrator, CN=u	sers, DC=cisco
*Manager Password:	••••	
* Confirm Manager Password:	••••	
* User Search Base:	CN=users, DC=cisco-irn,	DC=COM
* Attribute for User ID:	sAMAccountName 💌	
*Required fields		
	Back Next Skip	Cancel Help

Step 8 Configure the ICM translation route. These DNIS numbers need to be routable by your system (for example, enter a route in CUP SIP proxy). See Figure B-145.

Figure	B-145
riguic	0 140

Configure Unifi	ed ICM Trans	lation Route	e Targets				
- Enocify Unif		Dange					
* Starting DN	(S:	1200					
* Ending DNIS	S:	1202					
*Required field	s						
					((
				Back	Next Skip	Cancel	Help

Step 9 Configure the Cisco Unified Presence servers. See Figure B-146.

nchronize Presence Users	
Presence Servers	
* Primary Presence Server:	sip-1.cisco-irn.com
Secondary Presence Server:	sip-1.cisco-irn.com
*Presence Server Username:	bmcgloth
* Presence Server Password:	•••••
Test Connection	
Synchronization Schedule	
C Not Scheduled	Time 12 V AM V
● Every 5 minute(s) ▼	Day Sunday 💌
*Required fields	
Click Next to Synchronize Presence Users.	
	Back Next Skip Cancel Help

Step 10 Verify the summary. See Figure B-147.

Guided Initial Configuration Wizard Summary
You have successfully completed the following steps in the Initial Configuration Wizard:
 Welcome to Guided Initial Configuration Wizard Configure Primary Runtime Server Configure Primary Runtime Server Configure Unified ICM Translation Route Targets Configure Unified ICM Translation Route Targets Synchronize Presence Users Synchronize Presence Users
If you have skipped some steps, return to this wizard at any time by opening it from the System Management drawer.
Please note that you must supplement this initial configuration by completing some additional procedures. Click Help on this screen for details on full configuration.
Click Done to close the wizard and return to the Cisco Unified Expert Advisor Welcome screen.

- Step 11 In System Management tab, click on Synchronize Presence Users.
- **Step 12** Click on the **Synchronization** tab, click on **Synchronize Now**. Among other tasks, this will download the list of users from the CUP server. See Figure B-148.

Figure B-148

Connection.	Synchronization.				
Status					
Synchro	nization Task Status				
Synchro	nization Task Status Refresl	No Refresh	Go		
Current	Current Status: Idle				
Duration	1:				
Last Cor	mpletion Time:	12/07/2009	9:14:02 PM PST		
Last Res	sult:	Success			
AXL Web	Service Status				
Primary	Presence Server	Enabled	Enable AXL Web Service		
Seconda	ary Presence Server	Enabled	Enable AXL Web Service		
As of:		12/07/2009 9:15:44 PM PST	Refresh AXL Web Service		
Note: St	atus may be delayed by 10	seconds			
Synchroni Frequen	zation Schedule	Start Date and T	ime		
~ No	t				
Sc	heduled	Time 12 💌	AM 💌		
© Every 5 minute(s) ▼ Day Sunday ▼					
Manual Sy	nchronization				
Synchronize Now					
Click to st	tart the synchronization imm	ediately.			
* Synchronize Now saves the connection and schedule settings					
Required fi	elds				

Step 13 Add Expert Advisor users. In Daily Management tab, click on Expert Advisors.

Step 14 Click on Add New. Select the users from CUP. See Figure B-149.

Figure I	B-149
----------	-------

Ехр	Expert Advisors Items 1-5 of 5 Rows per page: 10 🔽 Go						
Filter: Presence ID 💌 Match if: Contains 💌 Go Clear Filter							
	Presence ID	First Name	Last Name	Locale	Unified ICM ID	Enabled	* Status
	jack2	Jack	Large	en_US	28	True	Valid 🛋
	<u>iill1</u>	Jill	Small	en_US	29	True	Valid
	<u>iill2</u>	Jill	Small	en_US	26	True	Valid
	<u>iohn1</u>	john	mini	en_US	25	True	Valid
	john2	John	Mini	en_US	24	True	Valid
Lice	Licenses Available: 0 Licenses Used: 5						
Add New Delete Enable Disable Page 1 of 1 14 4 D					of 1 🖪 🕘 🕨 🔊		
* Invalid means that the Expert Advisor no longer exists in the Presence Server.							

Step 15 Configure settings for the expert advisor users and click on **Add as Expert Advisors**. See Figure B-150.

Configure Expert Advisors				
Add as Expert Advisors 🖿 Back ? Help				
Expert Advisor Properties				
Copy Existing Expert Advisor Properties				
General				
Description:				
*Locale: English (United States)	(en_US)			
* Message Set: SystemDefined 💌				
I Enabled I Can Reject Contacts				
Selected Skills				
Skills	Items 0-0 of 0 Rows per page: 50 💌 Go			
Skill Name	Expert Advisor Competency Level			
No data to display				
Add Edit Edit All Delete	Page 0 of 0 🔣 🚽 🕨			
Selected Attributes				
Attributes	Items 0-0 of 0 Rows per page: 50 💌 Go			
Attribute Name	T Attribute Name Attribute Value			
No data to display				
Add Edit Edit All Delete	Page 0 of 0 14 4 🕨 🕅			
Add as Expert Advisors Back				
	c			

Figure B-150

Step 16 In Daily Management, select Skills. Click on Add New.

Step 17 Enter a name for the Skill and click on Add in the Expert Advisors section.

Step 18 Select the users that will belong to this skill and click on Add and Close.

Step 19 Click on Save. See Figure B-151.

Figure	B-151
--------	-------

Configure Skill					
📊 Save \prec Cancel (장 Refresh			? Help	
General					
General					
*Name:	Customer Service				
Description:	Customer Service Expert				
Expert Advisors					
Selected Expert Advisors			Items 1-4 of 4 Rows	per page: 50 💌 Go	
Presence ID	First Name	Last Name	Competency	Status	
🗖 john1	john	mini	50	Valid 🗖	
🗖 jill2	Jill	Small	50	Valid	
jack2	Jack	Large	50	Valid	
🗖 jill1	Jill	Small	50	Valid 🔽	
Add Edit Edit All	Delete		Page 1	of 1 🖪 🔍 🕨 🕅	
Assignment Queues					
List of Assignment Queues as:	sociated with this Skill.				
Assignment Queue Name I	n Use				
	<u> </u>				
*Required fields					
Save Cancel Refres	h				

- Step 20 Create an Assignment Queue. In Daily Management, select Assignment Queues. Click on Add New.
- **Step 21** Enter a Name for the assignment queue. Enter an incoming label. This label will need to be routable by the CUP SIP Proxy. Select the other appropriate settings, for simplicity use the Queue CTI-RP DN number. Click on **Save**. See Figure B-152.

Configure Assignment Queue		
🔚 Save 《 Cancel 🔇 Refre	sh	💡 Help
General Membership		
General		
*Name:	Expert Service	
Description:	Expert Level General Customer Service - High T	Touch
Unified ICM		
* ¹ Incoming Label:	1301 Test Uniqueness	
* Skill Group Peripheral Number:	47	
* Skill Group Peripheral Name:	Expert_Service	
Selection Strategy		
Queue ordering	 Longest Available Least Skilled Most Skilled 	
 Queue to Expert Spatial 		
Selected Attributes		Items 0-0 of 0 Rows per page: 50 💌 Go
Name	Description	Default Value
No data to display Add Delete		Page 0 of 0 10 0 10
Advanced		
Broadcast Number:	1 Broadcast Number greater than 5	0 can adversely affect performance.
* Offer Task Timeout:	30 (seconds)	
*Required fields ¹ Changes to the Incoming Label require	corresponding changes to Unified ICM.	
Save Cancel Refresh		

- Step 22 Click on the Membership tab.
- Step 23 Add the expert advisor users that should belong to this assignment queue. Click on Add and Close.See Figure B-153.

Figure B-153

pert Advisors	t Advisors						
Selected Expert Advisors Items 1-3 of 3 Rows per page: 50 💌 Go							
Presence ID	First	Name Last	Locale	Active	ence state(s) Inactive	Status	
john1	john	mini	en_US	Yes	No	Valid	<u> </u>
jack2	Jack	Large	en_US	Yes	No	Valid	
jill1	Jill	Small	en_US	Yes	No	Valid	-
Add Edit Edit All	Delete				Page 1	of 1 🔢 🔳 🛛	

- Step 24 Start the Expert Advisor runtime service.
- Step 25 Go to Serviceability > Control Center. Select the runtime server and click on Start. The status should be in "Running (in service)". See Figure B-154.

Figure B-154

Dev	ices		Ite	ms 1-1 of 1 Rows per page: 10 💌 Go
Filter	r: Name 🔽 Match if: Cont	ains 💌	Go Clear Filte	er
	Name	Host Address	Device Type	Status
0	<u>ea-1.cisco-irn.com</u>	192.168.81.101	Runtime	Running (in service)
Sta	art Shutdown Restart			Page 1 of 1 🚺 🗐 🕨 🕅

ICM Configuration

To configure ICM, complete the following steps:

- **Step 1** Select the PG for expert advisor and click on **Retrieve**.
- **Step 2** Click on Add Network Trunk group. Enter a name for the Network trunk group.
- Step 3 Click on Add Trunk. Provide a Peripheral name, and select Use Trunk Data for the Trunk count. See Figure B-155.

Network Trunk Group Explorer	
Select filter data PG EA_PG_2 Optional Filter Condition None Image: Cancel filter changes Save Eetrieve	Network trunk group Name: * EA_TRUNK Description Trunk for EA Trunk group
Hide legend Image: The trunk group Image: The trunk group <tr< td=""><td>Peripheral: * Peripheral number: * 0 Peripheral name: * Runtime_PG2_EA_TrunkGroup Name: * EA_PG_2.1.Runtime_PG2_EA_TrunkGr Extension: Trunk count: Use Trunk Data Configuration parameters: Description:</td></tr<>	Peripheral: * Peripheral number: * 0 Peripheral name: * Runtime_PG2_EA_TrunkGroup Name: * EA_PG_2.1.Runtime_PG2_EA_TrunkGr Extension: Trunk count: Use Trunk Data Configuration parameters: Description:
(2) Add Trunk group (2) Add Trunk (3) Add Trunk Multiple Instance: icm	Save Lep

- **Step 4** On the Unified ICM Configuration Manager, select **Explorer Tools > Skill Group Explorer**.
- **Step 5** Select the Expert Advisor PG, select **Retrieve**.
- Step 6 You should see the Skill Group/AssignmentQueue that was configured on Expert Advisor.
- **Step 7** Click on **Add Route** and add the route information.
- Step 8 Click on Save. This adds a new button to Add Peripheral target. Click on that button.
- **Step 9** Enter the DNIS that should be the same as the Incoming Label configured on Expert Advisor Operations Console.
- Step 10 Select the Expert Advisor Network trunk group. Click on Save.
- **Step 11** Click on **Add Label**. Select the Expert Advisor PIM. Enter the label that should be the same as the DNIS entered above.
- Step 12 Click on Save. See Figure B-156.

Select filter data	
Peripheral EA_PG_2_1	Skill Group Members Subgroup Mask Sub skill groups Skill Group Advanced
Optional Filter Condition Value	Media routing domain: * Cisco_Voice Peripheral number.* #47 Peripheral name.* Expert_Service.47
None	Name: * EA_PG_2_1.Expert_Service.47
	Available holdoff delay (sec): Priority Priority
Hide legend Skill group	Extension: ICM picks the agent
(2) Route (3) Peripheral target (0) John John John John John John John John	Route
(4) Laber	Skill group priority: 0
Jse the Add buttons to create new items.	Name: * SG1_R1
EA_PG_2_1.Expert_Service.47	Description
	Peripheral Target
	NIS: * 1301
	Description: incoming label configured in Expert Advisor
	Network trusk group: * EA TRUNK
	Label
	Routing client: * EA_PIM
	Label: * 1301
	Label type: * Normal
	Customer:
(4) Add Label	t

- Step 13 Configure the translation routes. On Configuration Manager, select Explorer Tools > Translation Route Explorer.
- Step 14 Select the PG for the Expert Advisor runtime server. Click on Retrieve.
- **Step 15** Click on Add Translation route. Enter a name for the translation route. Click on Add Route.
- **Step 16** Enter a name for the Route and click on **Save**.
- Step 17 Click on Add Peripheral target. Enter the DNIS to send the call to Expert Advisor runtime. Select the Network trunk group and click on Save.
- Step 18 Click on Add Label. Select the CVP Routing client, enter the label (same as the DNIS configured for the Peripheral target). Click on Save. See Figure B-157.
- **Step 19** Repeat those steps for other Translation Routes assigned to Expert Advisor.

Translation Route Explorer	
Select filter data PG EA_PG_2	Translation Route
Optional Filter Condition Value None Save Betrieve Cancel filter changes	Description: Type: * DNIS
Hide legend Hide legend (1) Translation route (2) Route (3) Peripheral target (4) Label Dick on an item to edit or view its contents. Use the Add buttons to create new items. ExpertAdvisor_TR ExpertAdvisor_TR ExpertAdvisor_TR_1	Route Name: * ExpertAdvisor_TR_1 Description Service name: EA_PG_2_1.Expert_Service.47 Peripheral Target DNIS: * 1200 Description:
DNIS:1200; NTG: EA_TRUNK DNIS:1200; NTG: EA_TRUNK ExpertAdvisor_TR_2 DNIS:1201; NTG: EA_TRUNK ExpertAdvisor_TR_3 DNIS:1202; NTG: EA_TRUNK DNIS:1202; NTG: EA_TRUNK UNASSIGNED	Network trunk group: * EA_TRUNK Label Routing client: * CUCM_RC Label: * 1200 Label type: * Normal Customer: icm Description: Image: Customer
CM Instance: icm	Save Qose Help

- **Step 20** Edit the Dialed Number for the Expert Advisor. This is the number that customer or agent will dial to reach an expert advisor user.
- Step 21 In Config Manager, go to List Tools > Dialer Number / Script Selector List and edit the Dialed Number for the CM Routing Client that was created previously.
- **Step 22** Go to the **Dialed Number Label** tab and click on **Add**.
- Step 23 Select all the translation routes configured for Expert Advisor and press OK. See Figure B-158.
| Figure I | B-1 | 58 |
|----------|-----|----|
|----------|-----|----|

Dialed Number / Script	Selector List				
Select filter data			Attributes	Dialed Number Mapping	Dialed Number Label
Routing client	<alb< th=""><th>•</th><th></th><th></th><th></th></alb<>	•			
Customer	<alb< td=""><td>•</td><td>Lat</td><td>ame Description</td><td></td></alb<>	•	Lat	ame Description	
Optional Filter	Condition	Value	12		
None	_	_	12	D2	
🗖 Save	<u>R</u> etrieve	Cancel filter changes			
- Dialed Number / Script Sele	ctor				
CUCM_RC.1000					
CUCM_RC.1301					
				Add Remove	

- Step 24 Click on Save.
- Step 25 In the Config Manager on the Admin Workstation open the Service Explorer option under Tools >Explorer Tools. Check that the Expert Advisor server has connected to the queue service. See Figure B-159.

Service Explorer	
Select filter data Peripheral EA_PG_2_1 Media routing domain All Optional Filter Condition Value Value None Value Save Retrieve Cancel filter changes Value Value Value Value Save Retrieve Cancel filter changes Value (1) Service (2) Route (3) Peripheral target (3) Peripheral target (4) Label Click on an item to edit or view its contents. Use the Add buttons to create new items. Vertex 4dd buttons to create new items. Value Value Value Value Value	Service Advanced Service members Media routing domain:* Cisco_Voice Image: Cisco_Voice Peripheral number: * 47 Peripheral name* [Expert_Service.47] Name: * EA_PG_2_1.Expert_Service.47 Configuration

Expert Advisor Script

Create the ICM Script for the Expert Advisor Queue on the AW by using the Script Editor software. shows a sample routing script. The logic that is followed for creating this script is as follows:

- **Step 1** Start the script with the start node.
- **Step 2** 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).
- **Step 3** Set the value of language in *Call.user.microapp.locale* as **en-us**.
- **Step 4** Set the value of input type (which is digits in this sample script) in *Call.user.microapp.input_type* variable to "**D**".
- **Step 5** Set the value of the *Call.user.microapp.app_media_lib* to **Custom**.
- **Step 6** After setting the variables send the call to IVR using **Send to VRU** node.
- **Step 7** Perform a DB lookup based on the calling number and/or caller entered digits for an account number.
- **Step 8** Use the Set Variable to save the values of the data retrieved from the Database as PeripheralVariables under the Call object type.
- **Step 9** Send the caller to Queue using the Queue to Skill Group, add the **EA_PG_2_1 Skill** group.
- Step 10 While the caller is in queue, play agent busy and music on hold .wav files in loop. See Figure B-160.





Trouble Shooting Tip

If using CUPC in the deskphone mode, you might see the following error message when the expert advisor is replying with a "**Yes**" that you will not see in the softphone mode. See Figure B-161.

Figure B-161

ExpertAdvisor@ipcc.vse.cisco.com (10:59 AM): Are you available to handle this contact? expert 1 (10:59 AM): y ExpertAdvisor@ipcc.vse.cisco.com (10:59 AM): Sorry, the system could not find your phone number. Please specify a phone number where you would like to receive the contact.

As a remedy, configure the Phone Numbers in the Expert Advisor page. See Figure B-162.

Phone Number Order		
Phone Number	Description	
5402001	Expert 1 Primary Phone Number	<u> </u>
Provided Phone Number	Phone Number Provided by the Presence Client	\overline{a}
		<u>≥</u>
		-
Edit Delete		
Phone Number Description		
5402001 Expert 1 Primary F	Phone Number Update Add	66

Database Lookup and Passing Data to the Expert

- **Step 1** Prepare your Database/CRM. Make sure you configure a primary key in your table.
- **Step 2** On the ICM Router servers execute the ICM setup utility (Run C:\icm\bin\ICMSetup.exe) and turn on Database Routing. See Figure B-163.

Figure B-163

Router Properties	×	
	Node Manager properties Production mode Auto start at system startup Duplexed Router Database routing Application gateway Remote Network Routing NAM ID: No system reboot on error Side Side Side Side Drive:	
	telp < <u>B</u> ack <u>N</u> ext > Cancel	0000

- **Step 3** On the ICM Router server, open the regedit utility and edit the registry key for the Database configuration as follows:
 - a. Locate HKEY_LOCAL_MARCHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\RouterA\Router\CurrentVersion\Configuration\Database.
 - **b.** For the SQLLogin key, enter the information of your database:

\\<ipaddress-or-name>\<Database_name>=(<username>, <password>)
Figure B-164.

Figure B-164

🍻 Registry Editor				
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>H</u> elp				
Elle Edit View Payorices Elep Image: Payorices Elep Image: Payorices Elep Image: Payorices Configuration Image: Payorices Image: Payorices Payorices Payorices Im	Name (Default) (AbandonTimeout) (Clugin)	Type REG_SZ REG_DWORD REG_SZ REG_DWORD REG_DWORD	Data (value not set) 0x00001388 (5000) \\192.168.45.141\MyTest=(vem,cisco) 0x0000005 (5) 0x0000015e (350)	
My Computer\HKEY_LOCAL_MACHINE\SOFTWA	RE\Cisco Systems, Inc.\	ICM\icm\RouterA\Rou	uter\CurrentVersion\Configuration\Database	Þ

Note

You need to do that only on one side. This setting will be automatically replicated to the other side.

- **Step 4** In ICM Configuration, open the DB Lookup Explorer.
- **Step 5** Enter a name for the Script Table. For side A and B, enter the DB server information with DB name and table as: \\<*IPorHostname*>\<DB>.<*Table*>. See Figure B-165.

🗞 Database Lookup Explorer	
_Select filter data	Database lookup: Script Table
Optional Filter Condition Value None Image: Save Image: Save Image: Save Image: Save Cancel filter changes	Name: CustometL0 Access type: SQL Side A: \\192.168.45.141\MyTest.Balances Side B: \\192.168.45.141\MyTest.Balances Description:
Hide legend (1) Script table (2) Column	Database lookup: Script Table Column
Click on an item to edit or view its contents. Use the Add buttons to create new items.	Description:
	Seve Lep

Step 6 In the ICM script, perform add a DB Lookup step to select the row you are looking for. For example, if the account number should match "1111", then enter the following information in the Database Lookup step. See Figure B-166.

🚸 DB Lookup Properties	×
Database Lookup Comment Connection Labels	
<u>I</u> able:	
CustomerLU	
Lookup value:	
"1111"	
T	
Formula <u>E</u> ditor	
OK Cancel He	lp g

Step 7 After a match is found other column data can be retrieved for this record. In the following example, we set the *PeripheralVariable1* to the AccountNumber column of the DB record, using the set step. Later on, with Expert Advisor, we will map this Peripheral Variable1 to an Expert Advisor variable, also called Expert Advisor attribute. See Figure B-167.

Figure B-167

Set Properties		×
Set Variable Comment	Connection Labels	
Object <u>type:</u>	Dbject: (No selection)	Variable: Periphera/Variable1
Array index:		
1		
		Formula <u>E</u> ditor
Vajue:		
Database.CustomerLL	I.AccountNumber	
		<u>F</u> ormula Editor
		OK Cancel Help

Step 8 On Expert Advisor OAMP, if you want to display this information to the expert, create new Attribute Definitions. Go to **Daily Management**, select **Attribute Definitions**. See Figure B-168.

- :	D 400
riaure	B-108

	Attrib	ute Definitions				
So Daily Management So Expert Advisors O of 31	4	Add New Delete			?	Help
Assignment Queues Message Sets	Attri	ibute Definitions r: Name 🔽 Match if: 📿 Co	Items 1-10 of 3	19 Row:	s per page: 10 💌] <u>G</u> o
Contact Attribute Sources		Name	Description	Data Type	System Defined	
Server Users		AccountNumber		String	No	<u>^</u>
		Balance		String	No	
		CustomerName		String	No	
		MMCA.ApplicationId	SystemDefined: The application ID in the OAMP configuration.	String	Yes	
		MMCA.ApplicationLastUpdate	System Defined: Last update of the application ID in the OAMP configuration.	String	Yes	
		MMCA.AssignmentQueueId	System Defined: The assignment queue ID in the OAMP configuration.	String	Yes	
		MMCA.AssignmentQueueLastUpdate	System Defined: Last update of the assignment queue ID in OAMP configuration.	String	Yes	
		MMCA.CallerAddress	System Defined: The address of the caller.	String	Yes	
F		MMCA.ConnectTime	System Defined The duration the contact was connected to the resource.	String	Yes	
		MMCA.ContactDisposition	System Defined: Disposition code associated with the terminated contact.	String	Yes	
	Ac	dd New Delete		Page	1 of 4 🖪 🖉 🕨	-

Step 9 Add new attribute definitions. Click on Disabled in the In Expert Advisor Client. See Figure B-169.

Figure B-169

	Configure Attribute Definition	
Expert Advisors Stalls	🔚 Save 🔇 Cancel 🔇 Refresh	? Help
Assignment Queues	General	
Message Sets	General Name: AccountNumber	
Scottact Attribute Sources Presence Client State Map Presence Server Users	Description:	
	*Data Type: String 💌	
	¹ Default Value:	
	Security Flags	
	In Log Files	
	Enabled - Appears as ocer text	
	C Macked - Dues not appear	
	S Masked Appears as masked text	
	In Expert Advisor Client	
	Charled - Appears as user (x) Charled - Does not annex (unless explicitly included in a token replacement string)	
	O Masked - Annears as masked text	
	C Explaided Stored as clear text	
	Disabled - Is not stored	
	O Masked - Stored as masked text	
	*Required fields	
	¹ Required if Data Type is Numeric.	
	Save Cancel Refresh	

Step 10 In Contact Attribute Sources, map the new Attribute Definitions to Variables you use in the ICM script. See Figure B-170.

Fiaure	В-	1	7	0	
	_	-	-	-	

<u>A</u>	Configure Contact Attrib	oute Source	
SP Daily Management Expert Advisors	🔚 Save 🔇 Cancel		? Help
Skins Assignment Queues	General		
 Message Sets Attribute Definitions Contact Attribute Sources Presence Client State Map Presence Server Users 	General *External Source: * ¹ External Name:	Unified ICM Call Variable 💌 PeripheralVariable1 💌	
	Description: * ² Attribute Name:	AccountNumber Add/Update	
	*Required fields ¹ External Name is case se ² Added/Updated with the	nsitive only for External Source Unified ICM ECC Variable. adjacent button.	
	Save Cancel Re	fresh	

Step 11 Modify the messages sent to the expert. Go the Daily Management > Message Sets. You can for example use the Clone functionality to clone the System Defined Message for English.See Figure B-171.

Figure B-171

	IM Message Sets					
So Daily Management So Expert Advisors	Add New Delete ? Help					
🤹 Skills Skills	IM Message Sets	IM Message Sets Rems 1-2 of 2 Rows per page: 10 💌 Go				
Message Sets	Filter: Name	• Match if: Contains 💌	Go Clear Filter]		
Sources	Name Name	Description	Default Locale	System Defined	Actions	
Presence Server Users	<u>SγstemDefined</u>	System Defined Message Set for English (US)	en_US [English (United States)]	Yes	Clone 🔺	
	VEM Custom	System Defined Message Set for English (US)	en_US [English (United States)]	No	Clone	
					v	
	Add New Delete			Page 1 of 1		

- **Step 12** Edit the new message set and choose the **To Expert** tab.
- Step 13 Edit the Contact Offer Request Notice.
- Step 14 Edit the Contact Offer Notice. See Figure B-172.

	Edit Message Set	
So Daily Management So Expert Advisors	🔜 Save 🔇 Refresh 🔏 Cancel 🧳	Help
🧙 Skills	- Edit Message Set	
Signment Queues Message Sets		
Attribute Definitions	*Name: VEM Custom	
Sources Sources Sources Sources	Description: System Defined Message Set for English (US)	
Server Users	Default Locale: English (United States) (en_US)	
	Configure Messages	
	* Name: VEM changes - English	
	Locale: English (United States) (en_US)	
	Format : HTML 💌	
	Even Event	
	To Expert	
	*Logon Greeting: Welcome to Cisco Expert Advisor %NCD:UserName%! 📑 Edit	
6	* Contact Offer Request Notice: Are you available to handle an Expert Assistance call for 📑 Edit	
	* Contact Cisco Expert Advisor Webpage Dialog	
	*Contact Configure Massages Edit	
	*Contact tate because Edit	
	Configure Messages in the text area and click Save.	
	CD: CustomerName%?	
	Device N Der, Please Cuit	
	* Contact	
	* Select Re	
	*Help:	
0	*System f Save Close Edit	
User Management	*System 1 Edit	
 W System Management 	* System (549
Bulk Management		- ACC

The dialogue with the Expert will then look like to what is shown in Figure B-173.



For more information on DB Lookup, refer to the *Scripting and Media Routing Guide for Cisco Unified ICM/Contact Center Enterprise & Hosted* and the *Administration and Configuration Guide for Cisco Unified Expert Advisor 7.6(1)* at the following URLs:

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html

http://www.cisco.biz/en/US/products/ps9675/prod_maintenance_guides_list.html

WebEx Access Anywhere

WebEx Access Anywhere is a simple method for an Agent to control the desktop and system that the customer used when contacting the agent from within the enterprise. The WebEx Access Anywhere service uses an agent installed on the remote system to allow connection and control from an Expert Agent without the customer having to connect to, navigate or share the system they are using via services such as WebEx meeting or Cisco Meeting Place sessions.

Step 1 To install the WebEx Access Anywhere agents on a system, login to the WebEx account. Select My WebEx from the tool menu and then click on My Computers. See Figure B-174.

	X						cisco
Welcome	Meeting Center	Event Center	Sales Center	More Services 🔻	🔵 My WebEx		Log Out
	My	WebEx Co	nputers			Welcome, john	1 mini
📷 My Meetings							?
Productivity T	ools Ca	mputer		Status	Application	Action	
My Computers	□ xpl	01		Available	Desktop	Connect	
🥪 My Files	Remov	e Set Up Co	mputer			Download man	ual installer
𝒞My Contacts							
🚷 My Profile							
🥩 My Audio							
🕢 My Reports				DOWEDED BY			
😪 Training				Cisco WebEx Technology			
强 Support			©2009 <u>WebE</u> ×	Communications, Inc Privacy Terms of Serv	All rights reserved. <u>rice</u>		

Step 2 Click on Set up Computer. Accept the Security Warning for ActiveX. See Figure B-175.

Figure B-175

Figure B-174

🔂 WebEx Access Anywhere Setup Wizard	×
Welcome to WebEx Access Anywhere Setup Wizard	
This wizard will help you to set up this computer for Access Anywhere.	
Click Next to continue.	
<back next=""> Ca</back>	ncel

Step 3 Click Next.

Step 4 Enter the Computer name and WebEx Account Info and click Next. See Figure B-176.

Figure B-176

😴 WebEx Access Anywhe	re Setup Wizard	×
Account Information		
Please enter a nickname	for this computer.	
Computer name:	xp03-Branch 123	
Please provide your Web	Ex account information.	
Note: An email message automatically sent to yo this computer.	containing your account information was u once you downloaded Access Anywhere to	
_ WebEx account info	rmation	
URL:	ciscocmo-dev.webex.com/cis	
User name:	john1	
Password:	******	
l Please provide the URL f	or your WebEx service.	
	< Back Next> Cancel	22.82.47

Step 5 Click Next.

Step 6 For Virtual Expert Kiosks in an Enterprise Branch configure the session options to enable both the Expert and the customer to access and control the System at the same time. Click Next. See Figure B-177.

Γ	Session options
	Use full-screen view by default
	Disable this computer's keyboard and mouse
	Make this computer's screen blank
	End this session after it remains idle for 45 Minutes
	Disable pop-up messages
	Lock computer after session ends

Figure B-177

Step 7 Configure access for the entire Desktop and click Next. See Figure B-178.

💕 WebEx Access Anywhere S	etup Wizard	×
Applications		
On this computer, access: © Entire desktop ⊂ O Specific applications		
	Add	
	Rename	
	Remove	
,		
	<back next=""> Cancel</back>	010000

Step 8 Set the Access code for this system and click **Next.Figure B-179**.

Figure B-179

💕 WebEx Access Anywhere Setup Wizard	×
Authentication	
To provide greater security for your remote computer, select a method of authentication.	
Method • Access code • Phone	
Vour access code	
Access code: *****	
Confirm access code: ******	
Note: Combine special characters (\$, @, %), numbers (1, 2, 3), and letters (a, b, c) to create a secure access code.	
	_
< Back Next> Cancel	2000ED

Step 9 With setup completed, click **Finish**. See Figure B-180.

Figure	B -'	180
--------	-------------	-----

💕 WebEx Access Anywhere Setup Wizard	×
Setup Complete	
You have successfully installed the Access Anywhere agent software and set up this computer for Access Anywhere.	
To access this computer remotely: - it must be connected to the Internet - the Access Anywhere agent must be running	
To start the Access Anywhere agent now, click Finish.	
< Back	Finish

Step 10 The newly added system will be listed in the My WebEx Computer table and the WebEx Access Anywhere agent will be running in the System Task Tray waiting for a connection. See Figure B-181.

Figure	B-1	81
--------	-----	----

