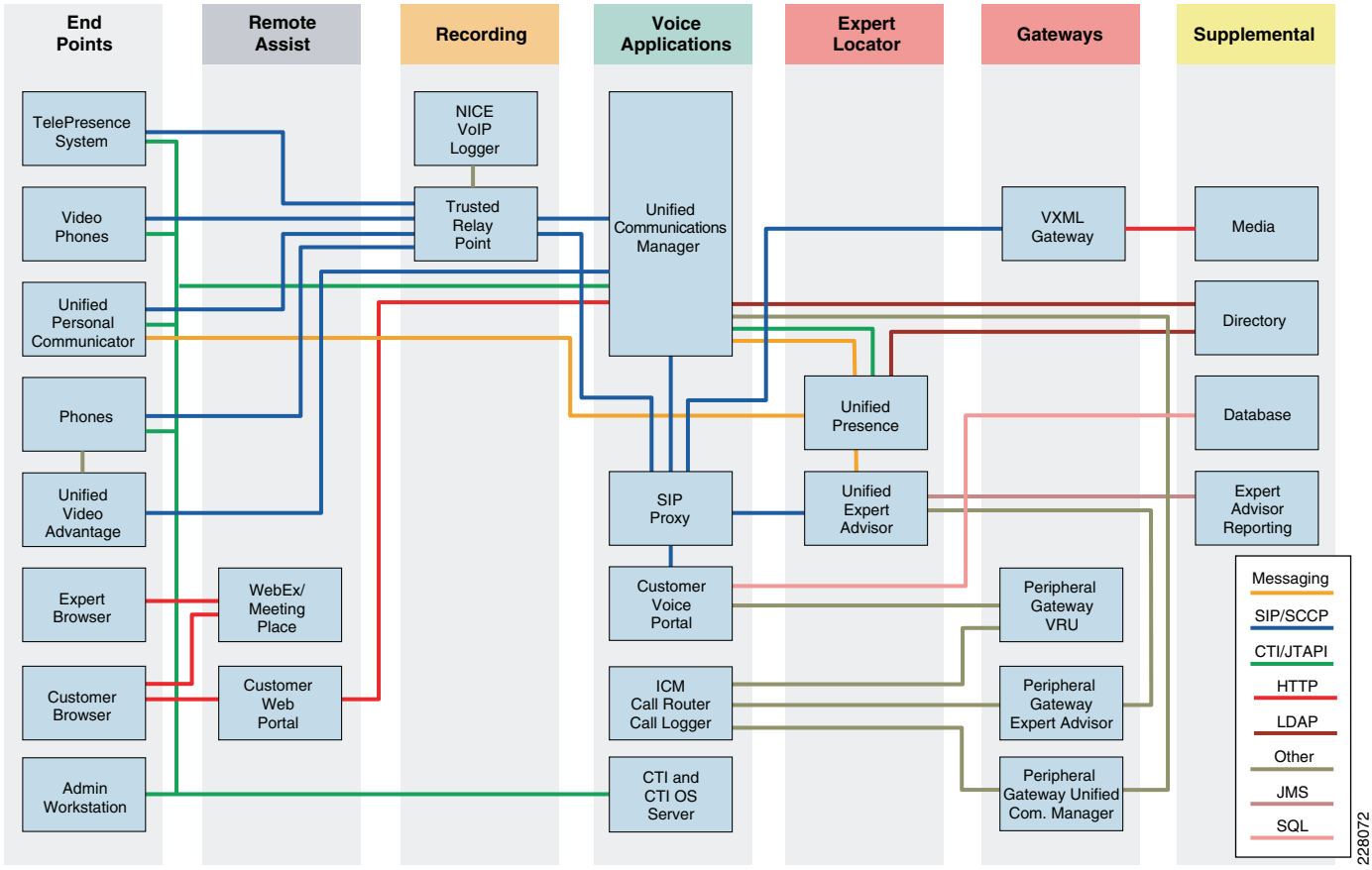
APPENDIX **B**

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:

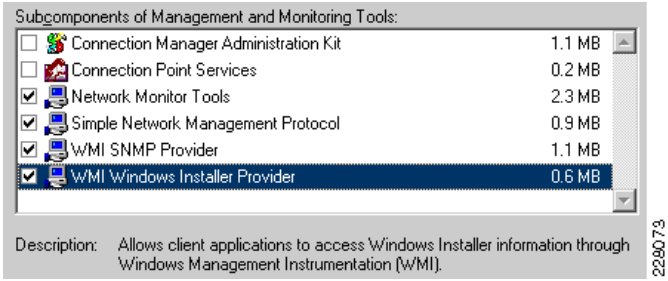
- Cisco Unified Communication Manager (CUCM)
- Cisco Unified Intelligent Contact Management (CUICM)
- Cisco Unified Cisco Voice Portal (CUCVP)
- Cisco Voice Gateways and VXML Gateways
- Cisco Unified Expert Advisor
- Cisco Unified Presence and SIP Proxies
- Cisco Unified TelePresence
- Cisco Unified 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



- 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_guides_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_list.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

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

Note 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), l 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.

Note 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

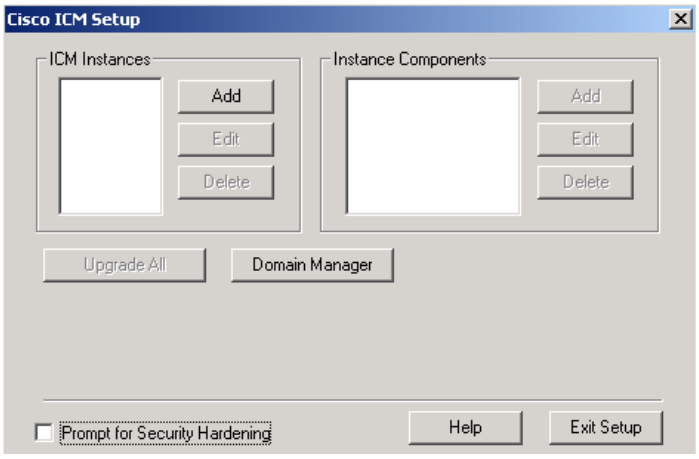
- Before any ICM components can be installed and ICM instance must first be created
- Before an instance can be selected the proper entries must first be created in the domain using the Domain Manager

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.

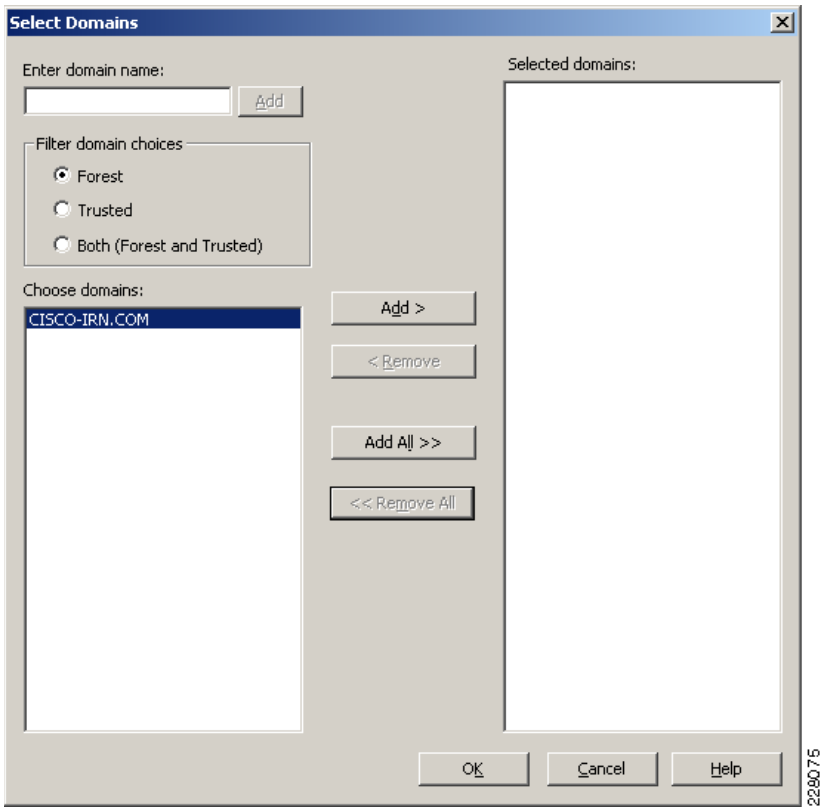
Step 2 Click the **Domain Manager**. See Figure B-3.

Figure B-3 Domain Manager



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

Figure B-4 Selecting Domain

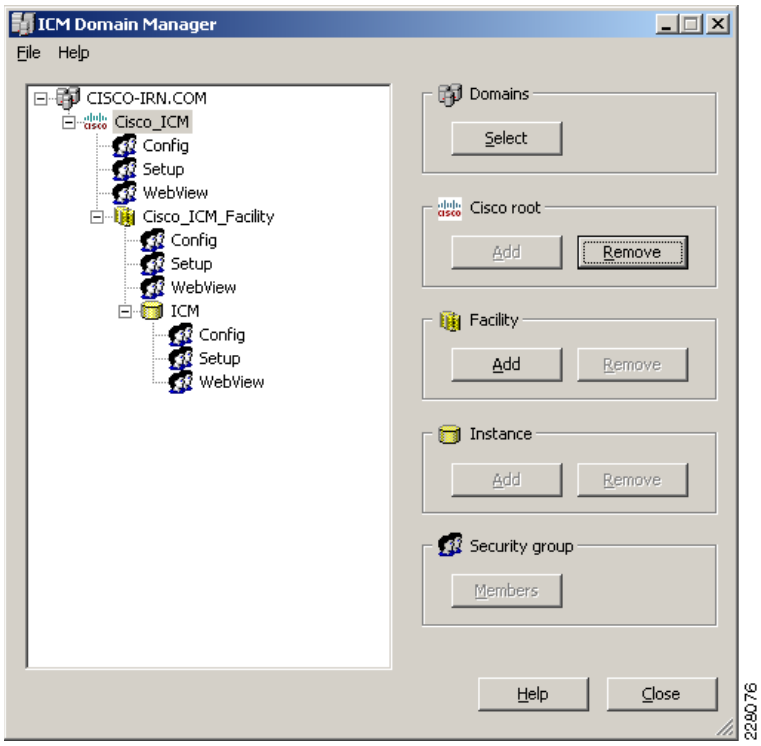


Step 4 After the domain is selected, click **Add** it under the Cisco root section. Enter an appropriate name such as **Cisco_ICM** and click **OK**.

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.

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.

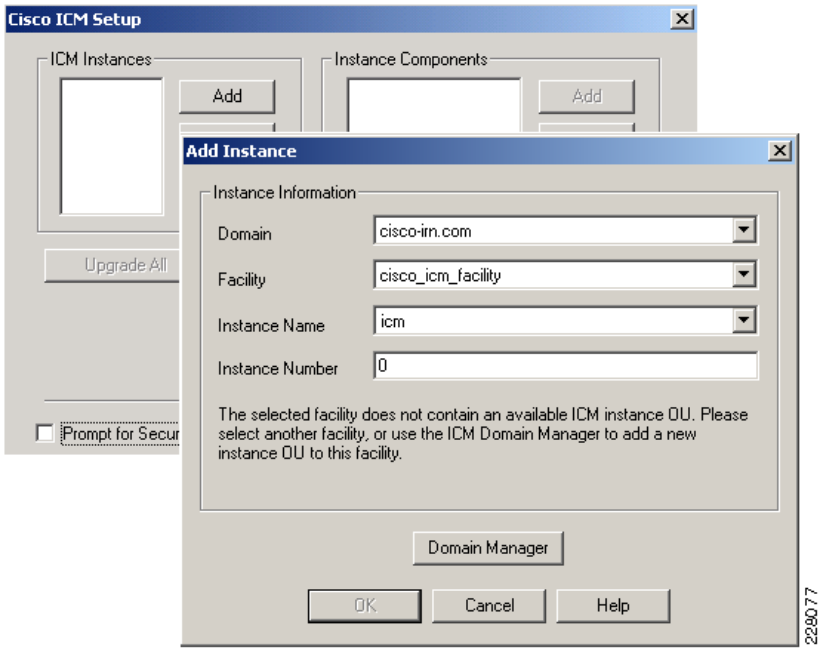
Note The ICM Instance Name is the name of the Instance Organizational Unit.

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

Note 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 Instance



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:

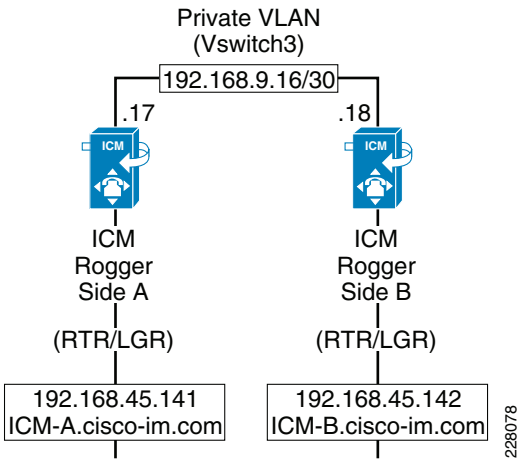
http://www.cisco.com/en/US/docs/voice_ip_comm/cust_contact/contact_center/icm_enterprise/icm_enterprise_7_5/installation/guide/icm75instl.pdf

Install the Router and Logger

Call Router Installation

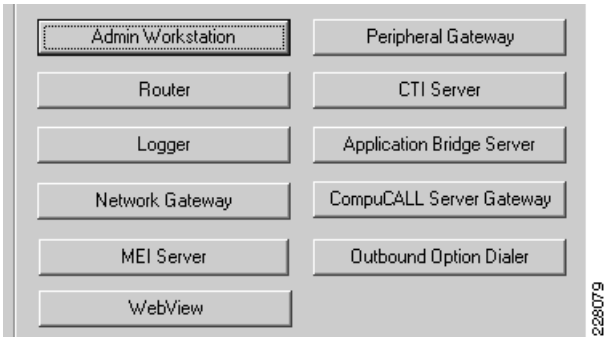
The CallRouter (generally referred to in this document simply as the *Router*) is the component that contains the contact routing logic and makes all routing decisions. It receives contact routing requests and determines the best destination for each contact. It also collects information about the entire 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.

Figure B-7 Router and Logger Servers



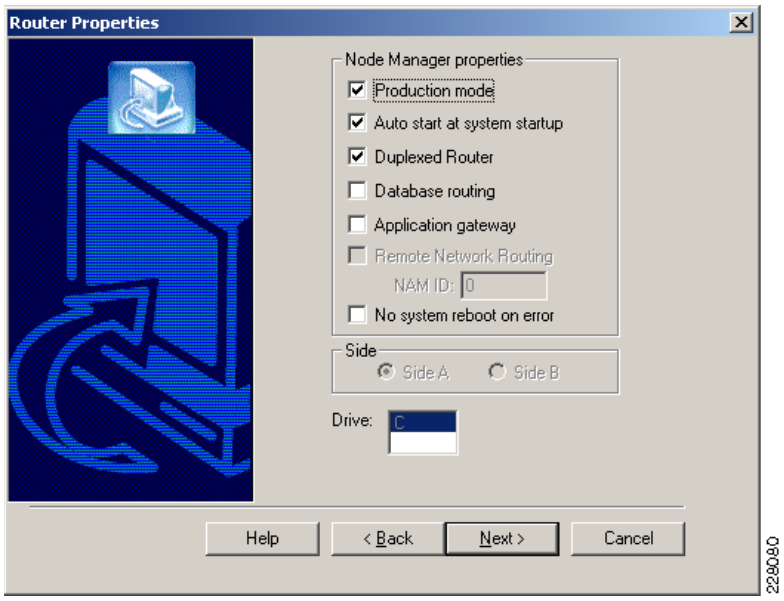
Step 1 In the ICM Setup application, click the **Add** button on the right under **Instance Components**. See Figure B-8.

Figure B-8



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

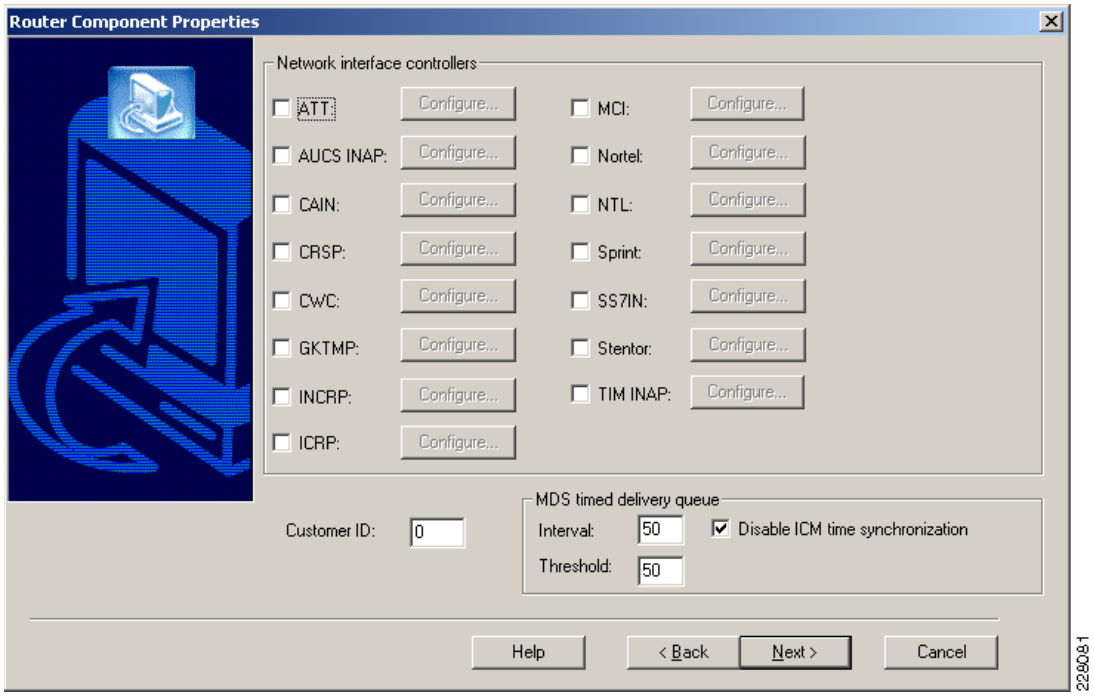
Figure B-9



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.

Figure B-10

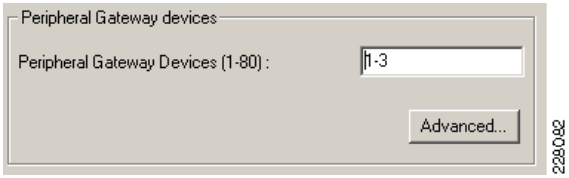


Step 3 Click **Next**.

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.

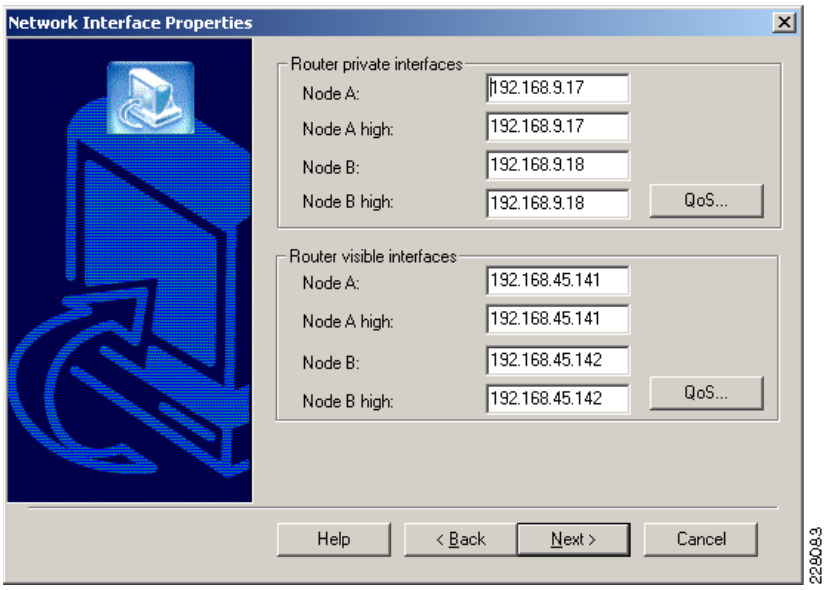
Figure B-11



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.

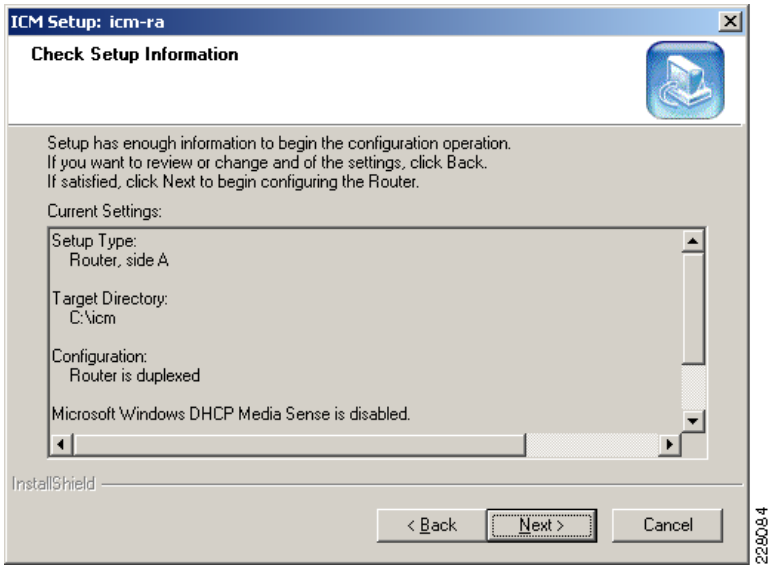
Figure B-12



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.

Figure B-13



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.

Figure B-14

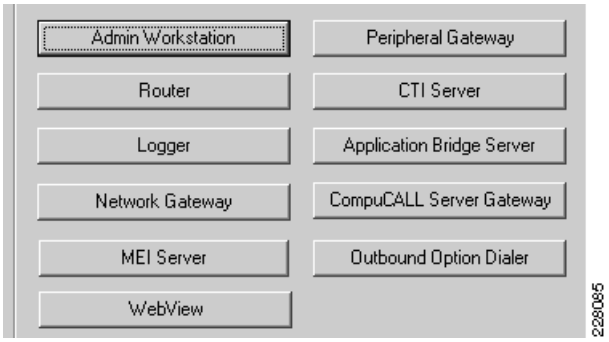
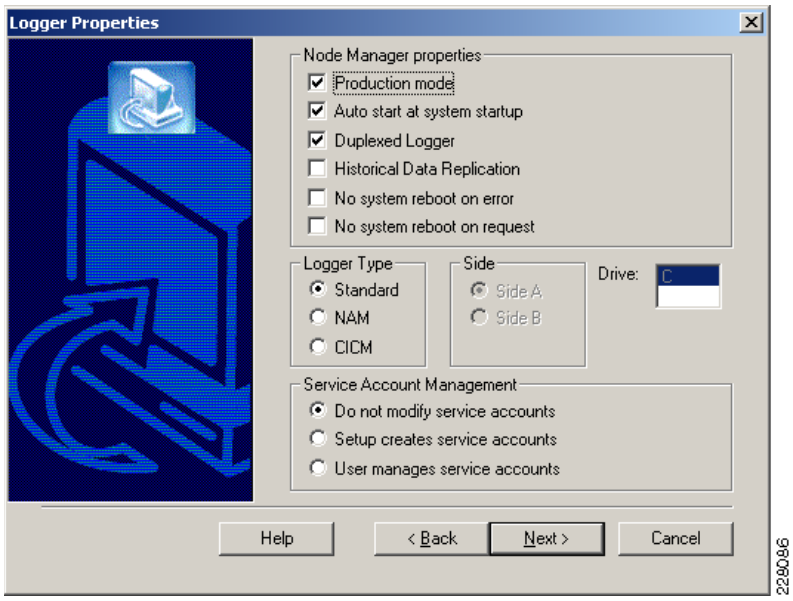
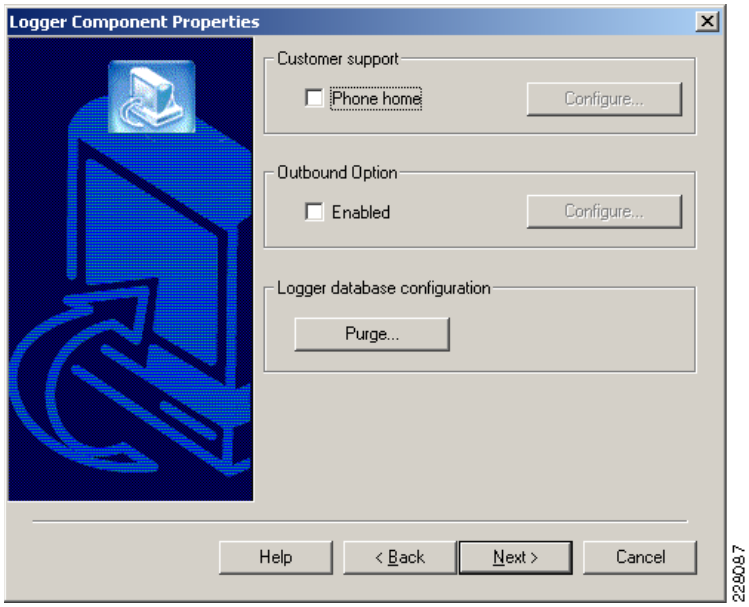


Figure B-15



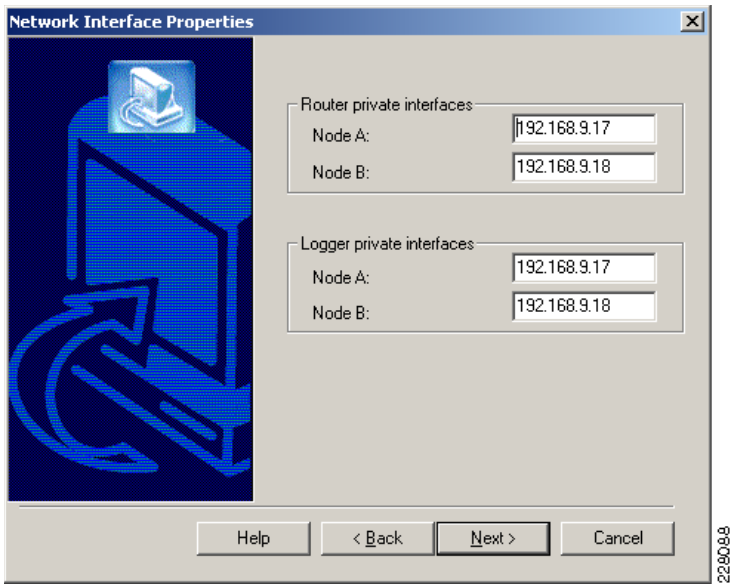
Step 7 Select production, Auto startup and Duplexed logger options, then click **Next**. See Figure B-16.

Figure B-16



Step 8 Click **Next**. See Figure B-17.

Figure B-17



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.

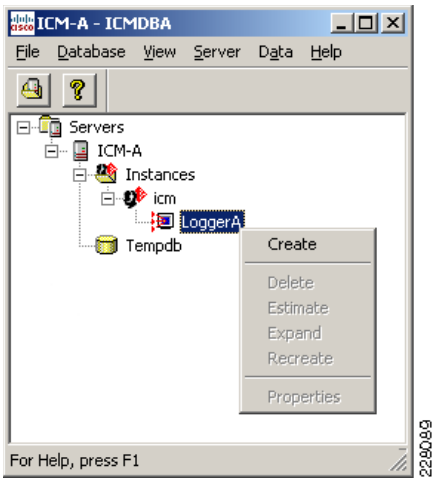
Create ICMDB on Logger

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.

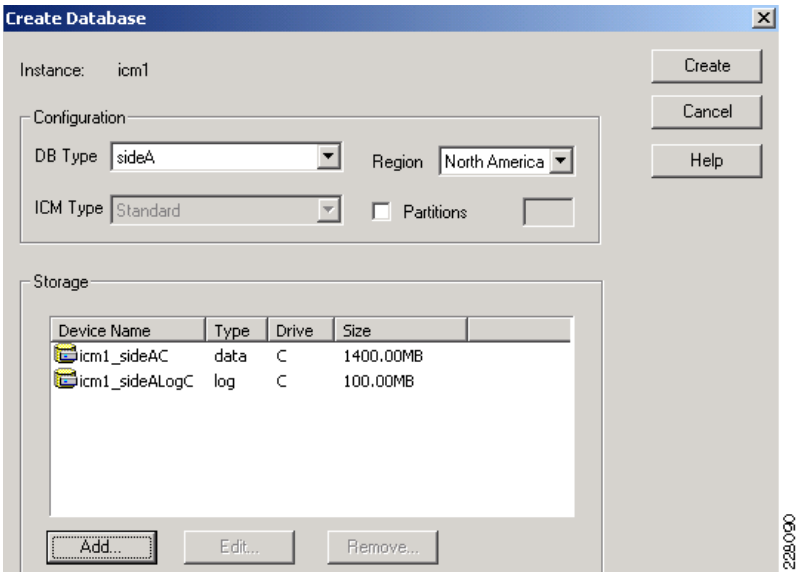
Figure B-18



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.

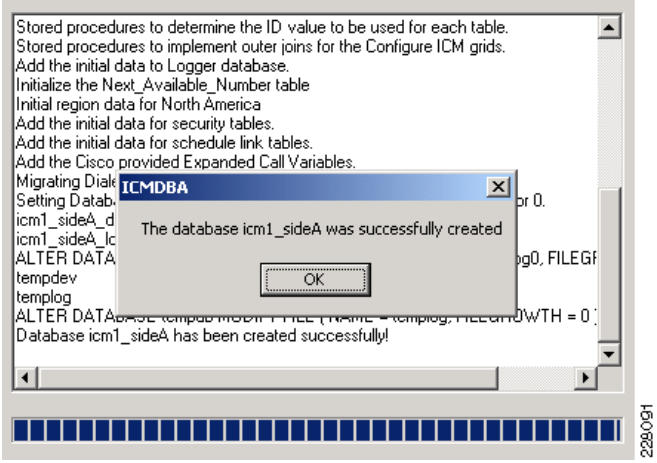
This time all the necessary changes have been made, you will be able to create the database. Now add the data and log databases to the list and create the database. See Figure B-19.

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**.

Figure B-20

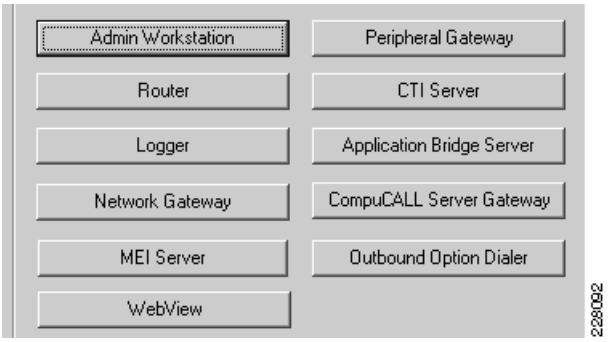


Installing the Admin Workstation

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.

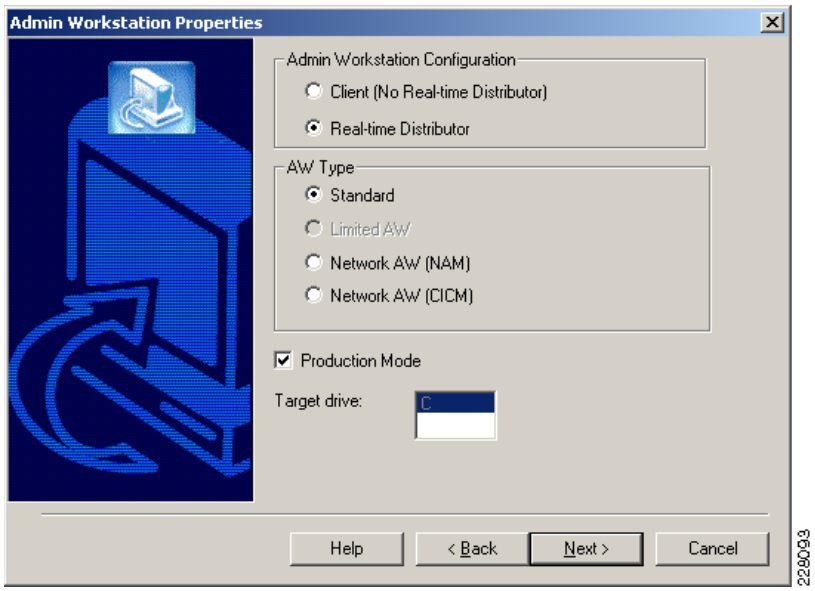
The Admin Workstation (AW) is the human interface to the ICM software. It serves as a control console where you can monitor agent and contact center activity and change how the ICM software routes contacts. For example, you can use the Admin Workstation to configure the ICM contact center data and to 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.

Figure B-21



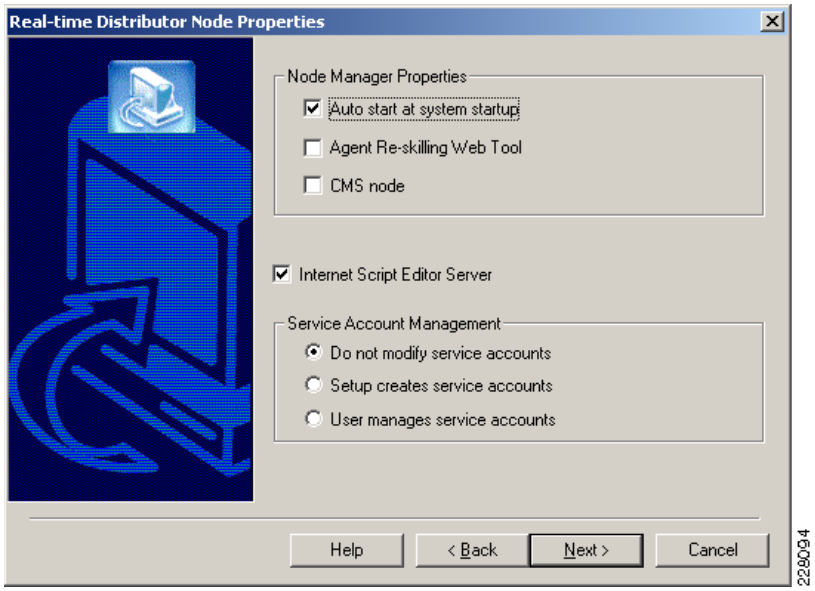
Step 1 From the ICM Setup applications, select **Add** for the ICM instance and then "**Admin Workstation**". See Figure B-22.

Figure B-22



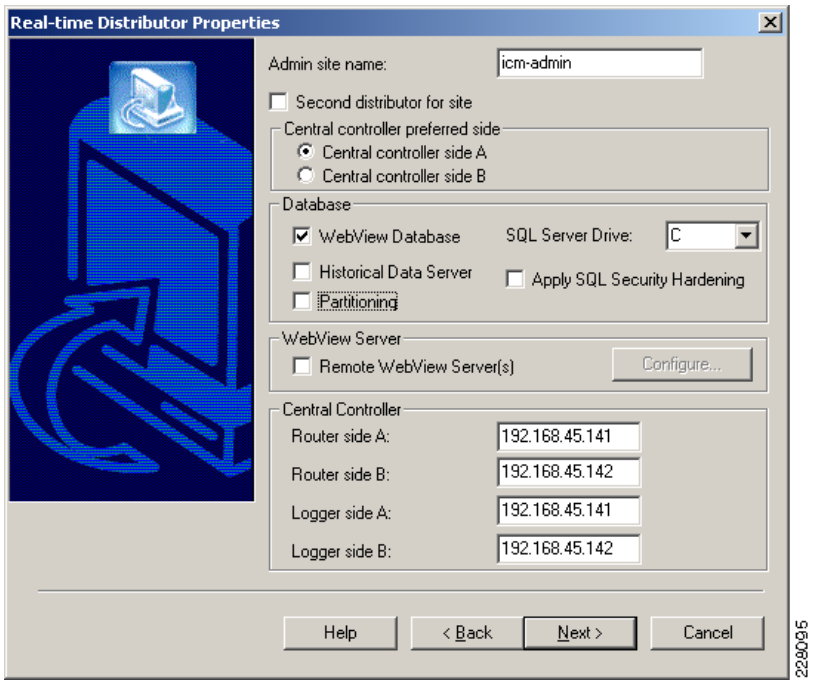
Step 2 Select **Next**. See Figure B-23.

Figure B-23



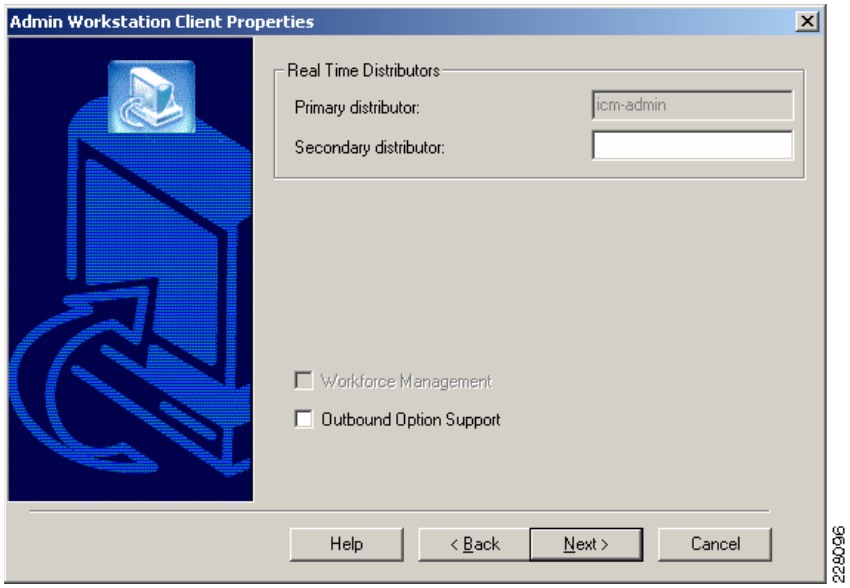
Step 3 Select **Next**. See Figure B-24.

Figure B-24



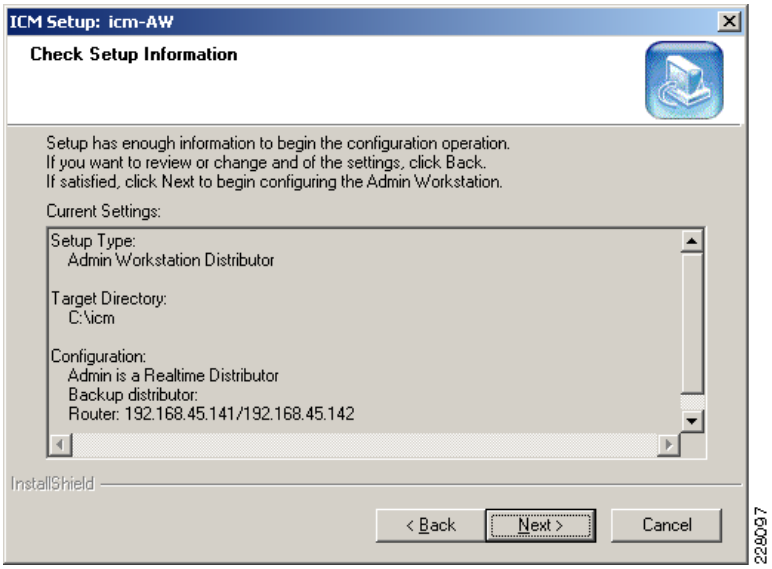
Step 4 Select **Next**.See Figure B-25.

Figure B-25



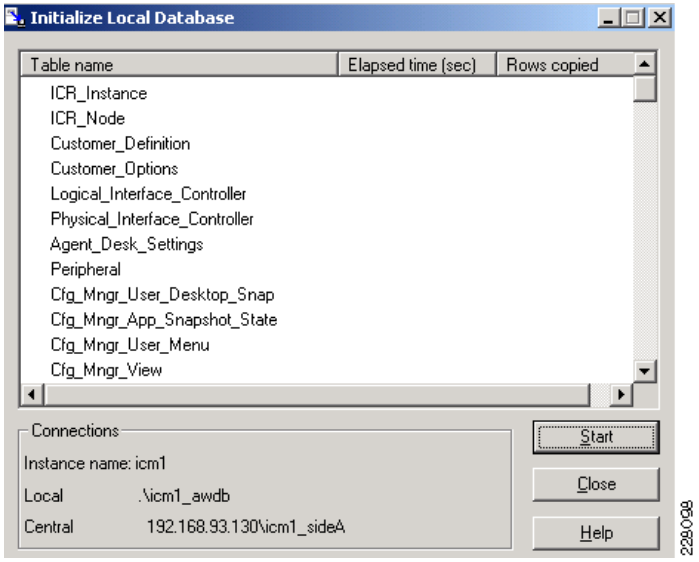
Step 5 Verify Setup parameters and select **Next** to finish. See Figure B-26.

Figure B-26



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



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**.

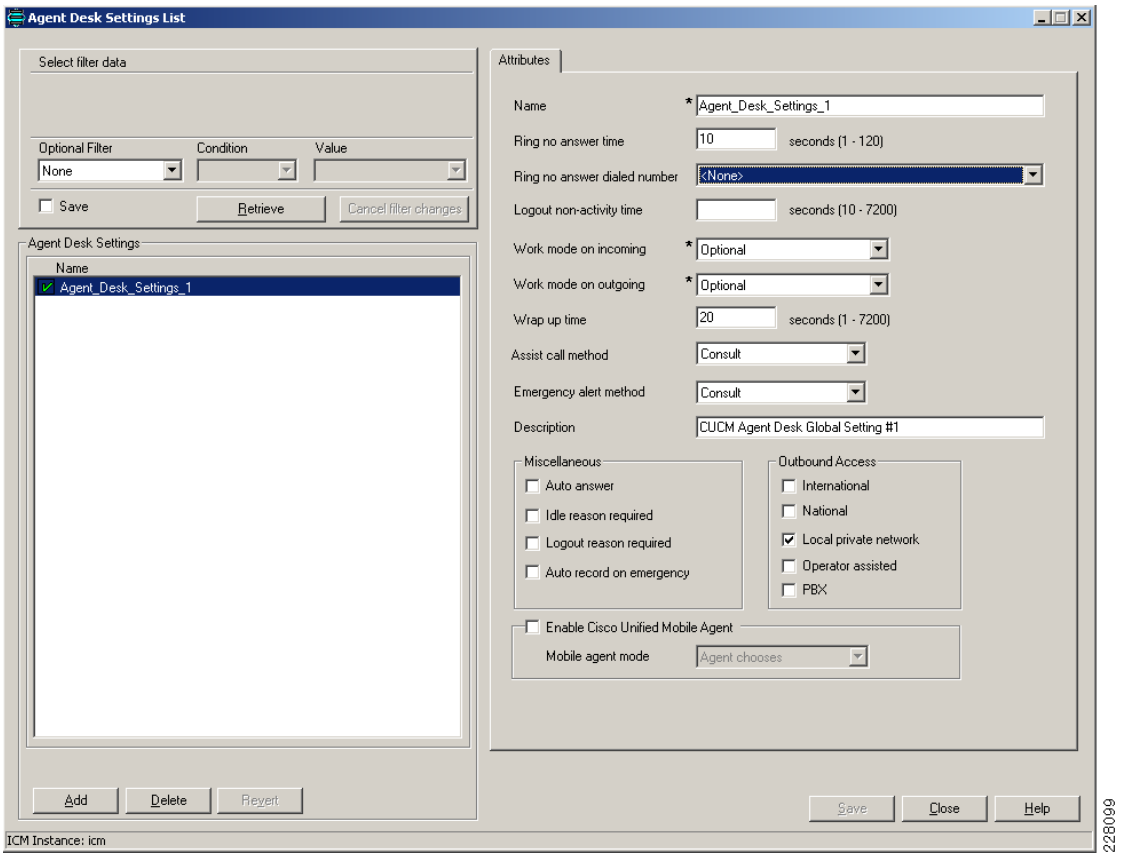
Step 6 Enter a proper description.

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



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**.

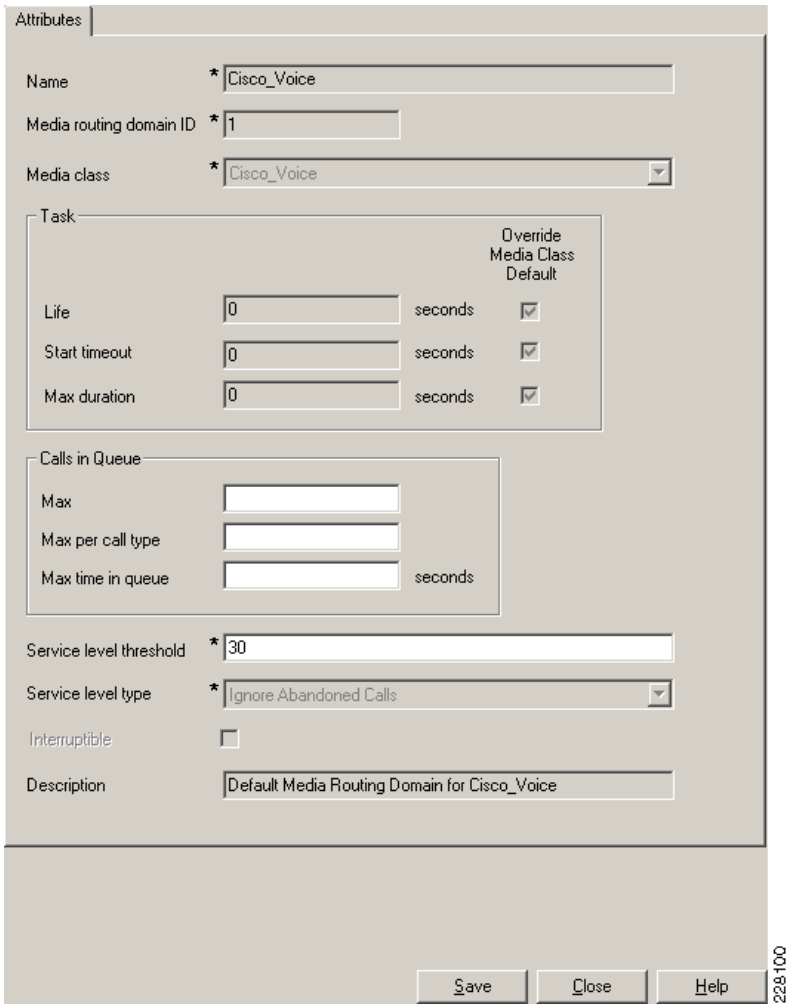
Step 5 Enter an appropriate list name such as **Cisco_Voice**.

Step 6 Enter a proper description.

Step 7 Set the Media Class to **Cisco_Voice**.

Step 8 Click **Save**. See Figure B-29.

Figure B-29



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.

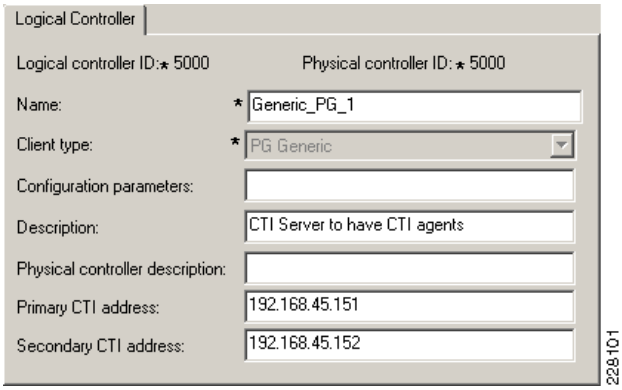
Step 7 Set the client type to **PG Generic**.

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



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**.

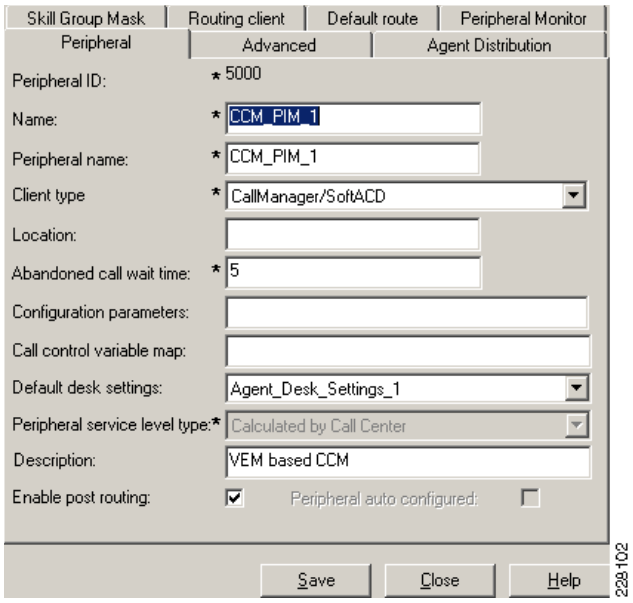
Step 6 Enter a proper description.

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.

Figure B-31



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**.

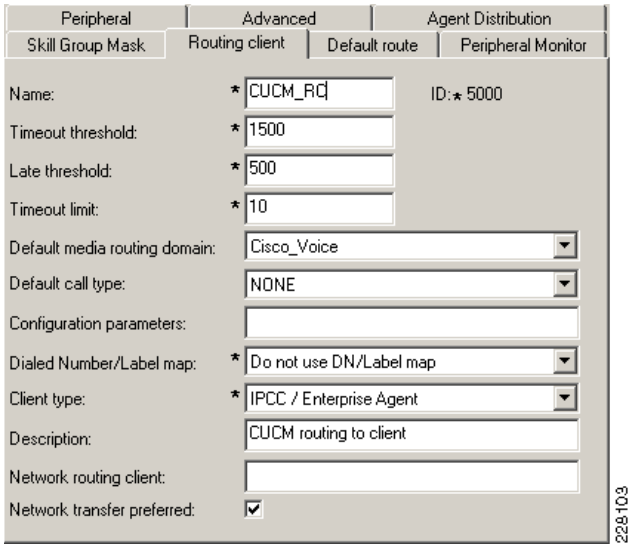
Step 2 Select the Client Type as **PCC/Enterprise Agent**.

Step 3 Select the Default media routing domain option to **Cisco_Voice**.

Step 4 Enter a proper description.

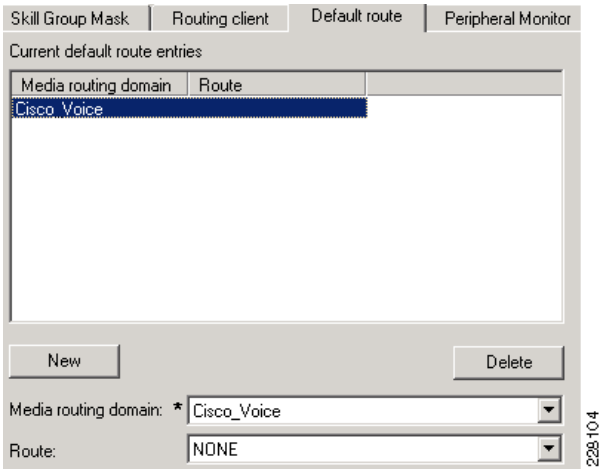
Step 5 Click **Save**. See Figure B-32.

Figure B-32



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

Figure B-33



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**.

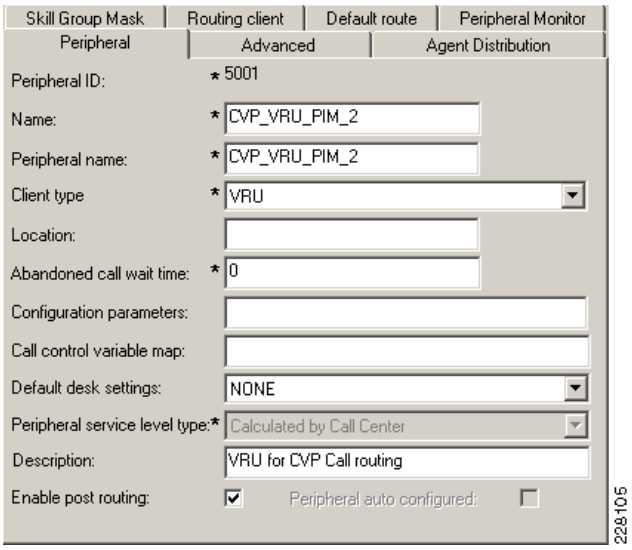
Step 6 Enter a proper description.

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.

Figure B-34



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**.

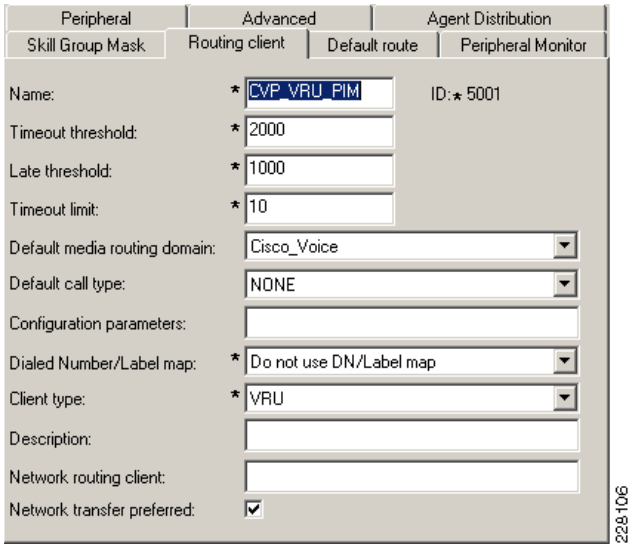
Step 2 Select the Client Type as **VRU**.

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



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.

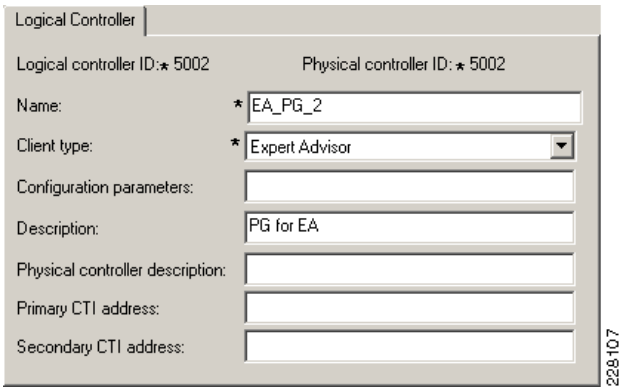
Step 7 Set the Client Type to **Expert Advisor**.

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



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.

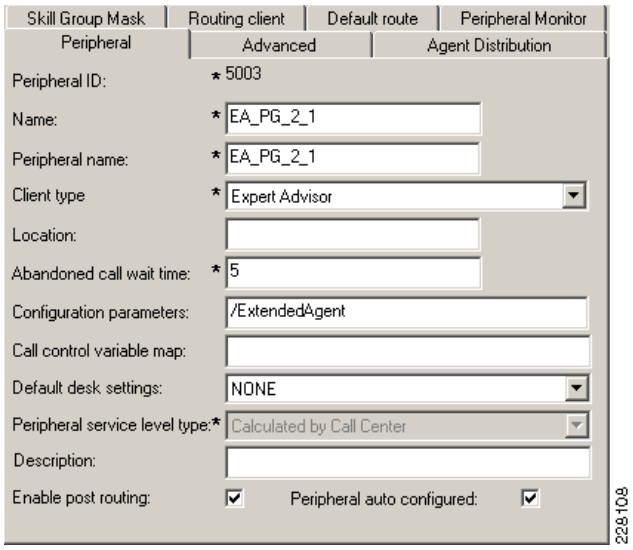
Step 8 Check the **Enable post routing** option.

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.

Figure B-37



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

Step 1 Enter an appropriate peripheral name such as **EA_PIM**.

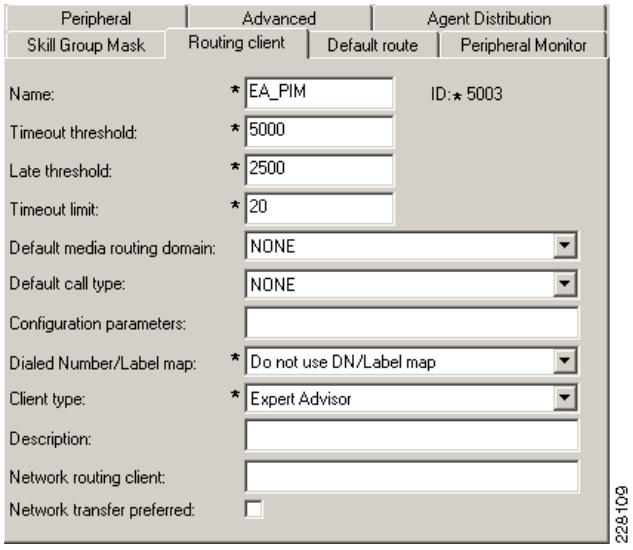
Step 2 Select the Client Type as **Expert Advisor**.

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



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.

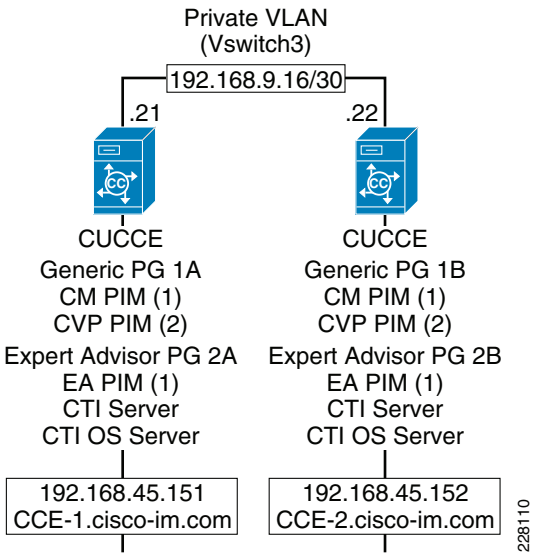
To configure a PG, you must know the visible network addresses for the CallRouter machines. If the PG is duplexed, you must know the visible and private network addresses of its duplexed peer.

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.)

Note 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.

Figure B-39 Cisco Unified Contact Center Servers



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.

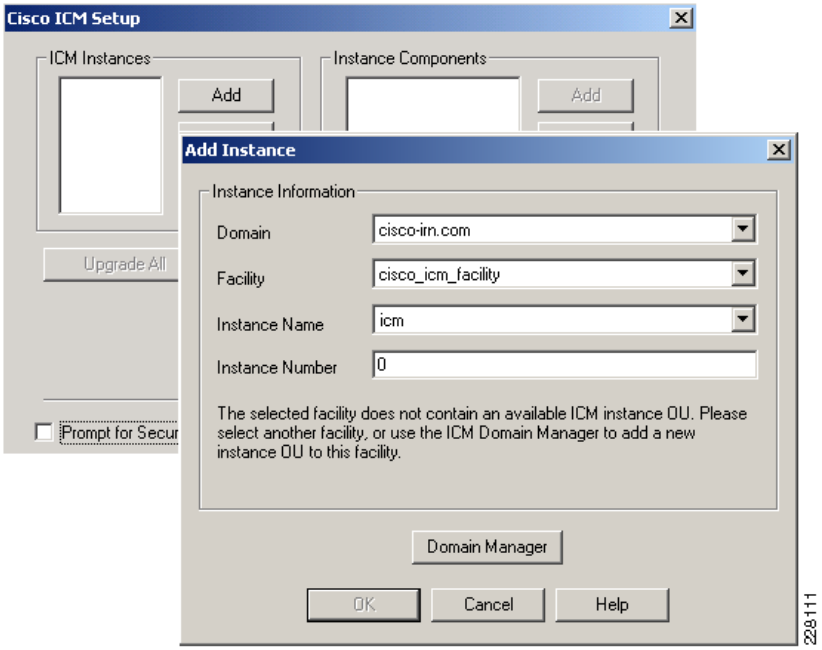
Note The ICM Instance Name is the name of the Instance Organizational Unit.

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**.

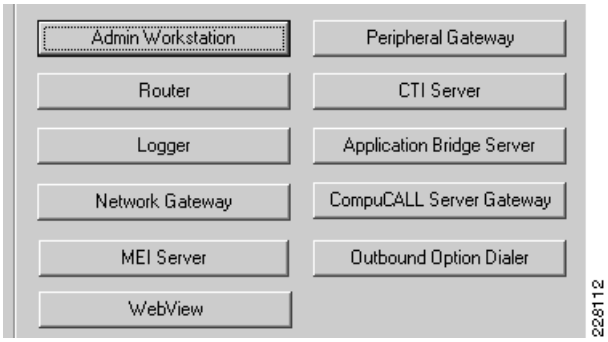
Figure B-40



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.

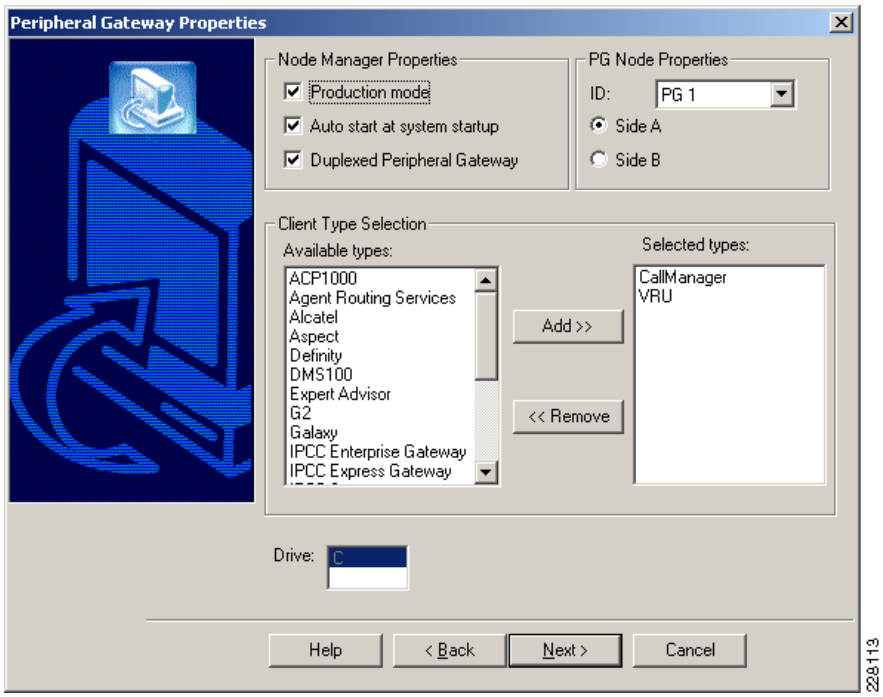
e. Select the following client types and click the **Add** button:

   – CallManager

- VRU

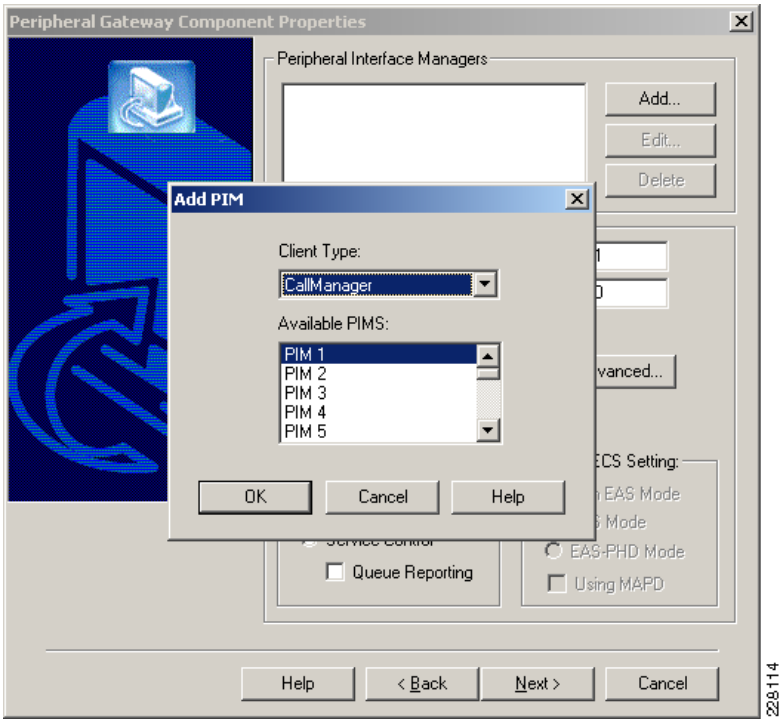
f. Click **Next**. See Figure B-42.

Figure B-42



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.

Figure B-43



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.

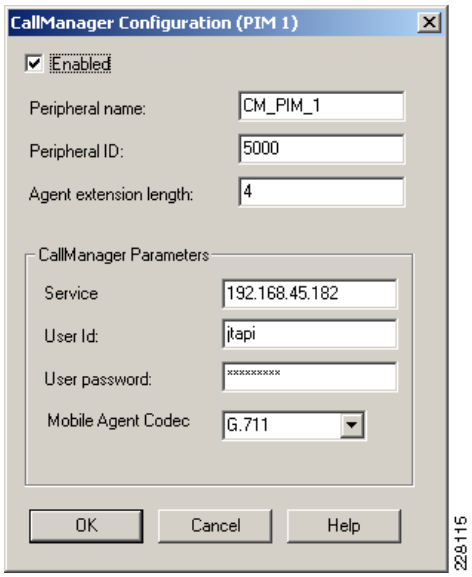
d. Specify the appropriate agent Extension length for DN's on the Cisco Unified Communication Manager (this is critical as additional digits are added for call handling to CVP and call handoff will fail when mismatched).

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).

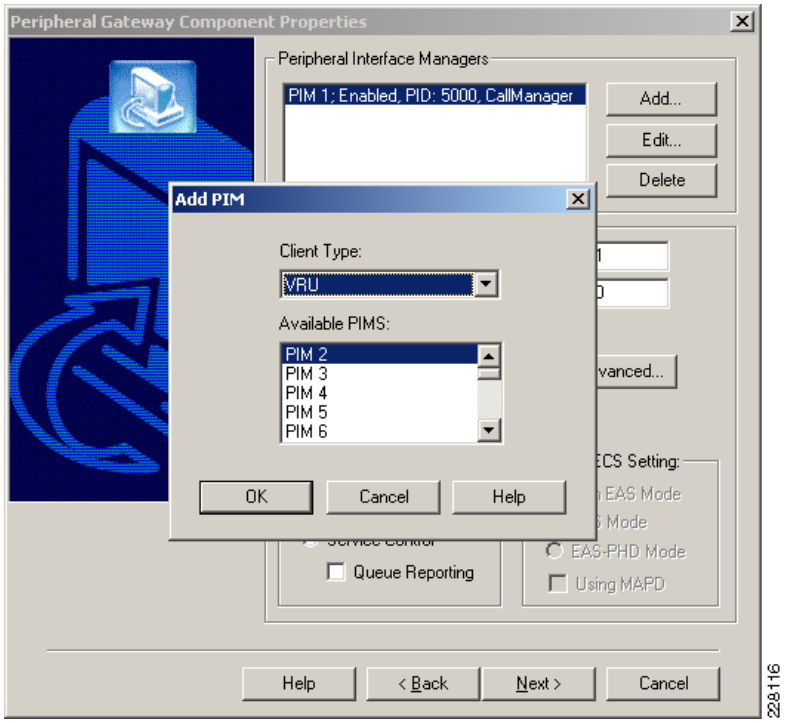
g. Click **OK**. See Figure B-44.

Figure B-44



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



Step 6 In the PIM Configuration dialogue, configure the PIM as follows:

a. Select **Enable**.

b. Enter an appropriate Peripheral name.

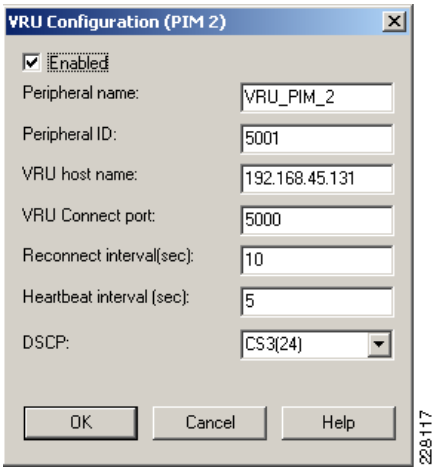
c. Enter the Peripheral ID that was assigned by the Configuration Manager on the Admin Workstation.

d. In the VRU Hostname enter the IP address of the CVP Server.

e. Enter VRU connection port.

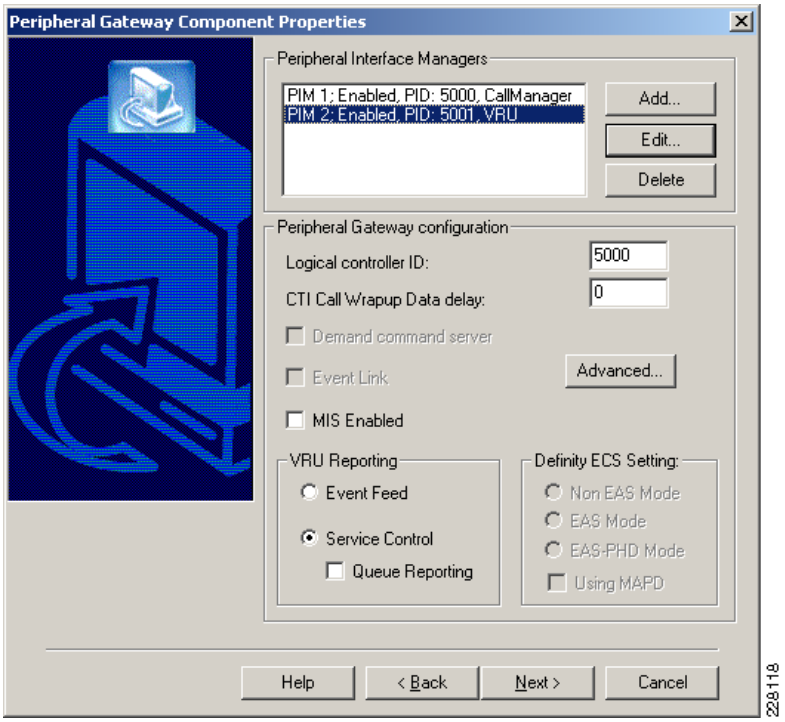
f. Click **OK**. See Figure B-46.

Figure B-46



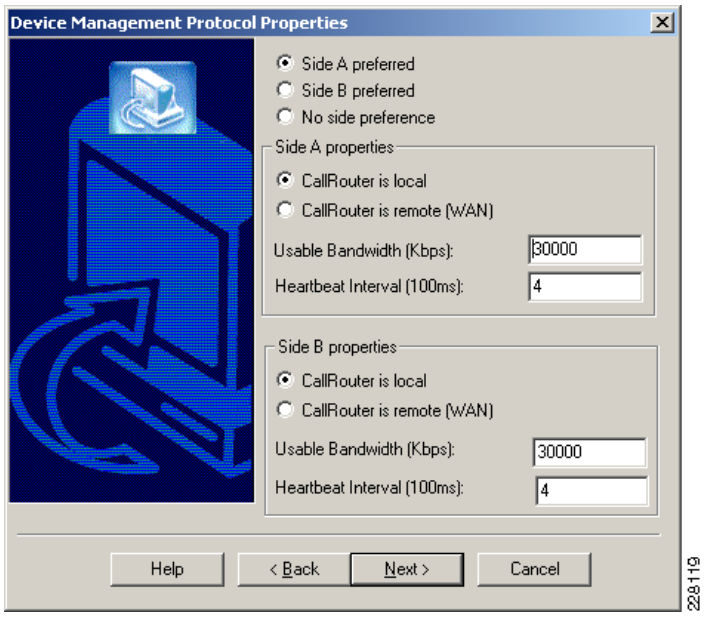
Step 7 Back on the Peripheral Gateway Component Properties enter the Peripheral Gateway Logical controller ID that was generated by the Configuration Manager on the Admin Workstation and click **Next**. See Figure B-47.

Figure B-47



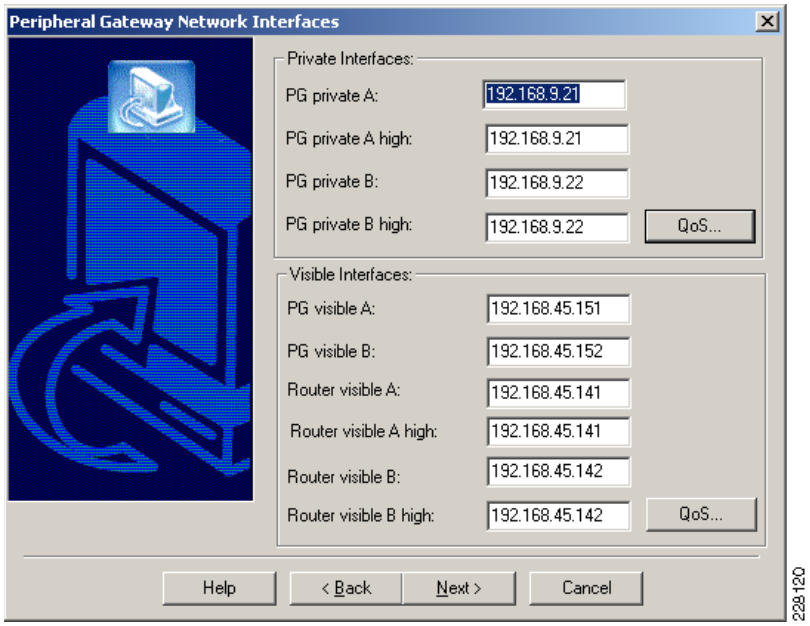
Step 8 On the Device Management Protocol Properties set **Side A preferred** option and click **Next**. See Figure B-48.

Figure B-48



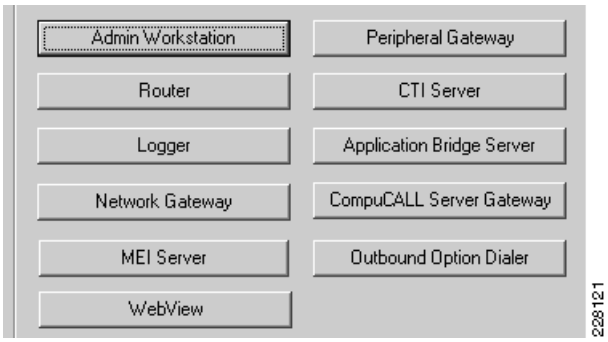
Step 9 Enter the name or IP addresses for the Visible and Private Interfaces of the PG and Router. Optionally, enable QoS for these interfaces as desired. Click **Next**. See Figure B-49.

Figure B-49



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.

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**.

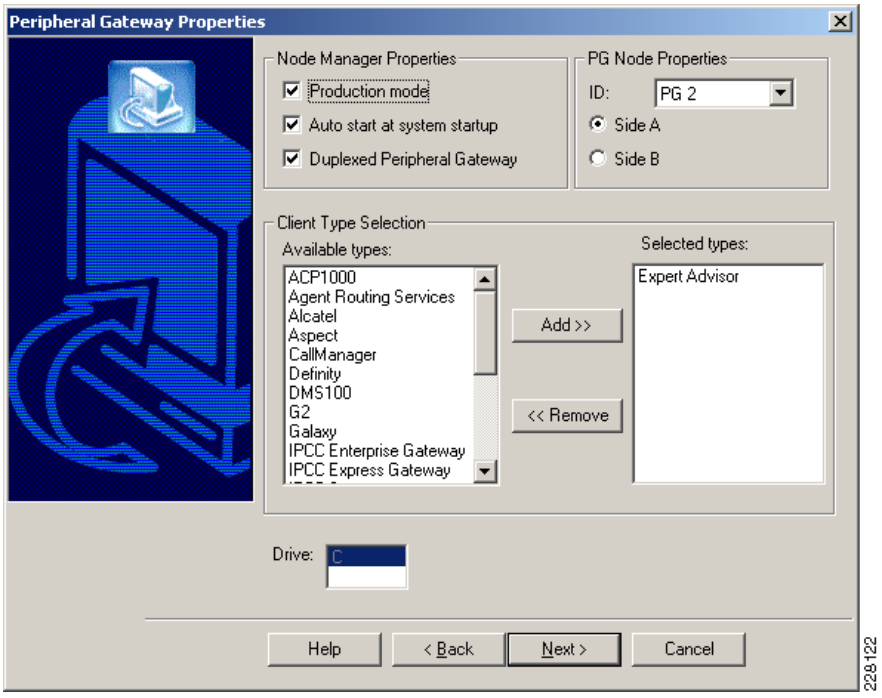
c. Check the duplexed Peripheral Gateway.

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.

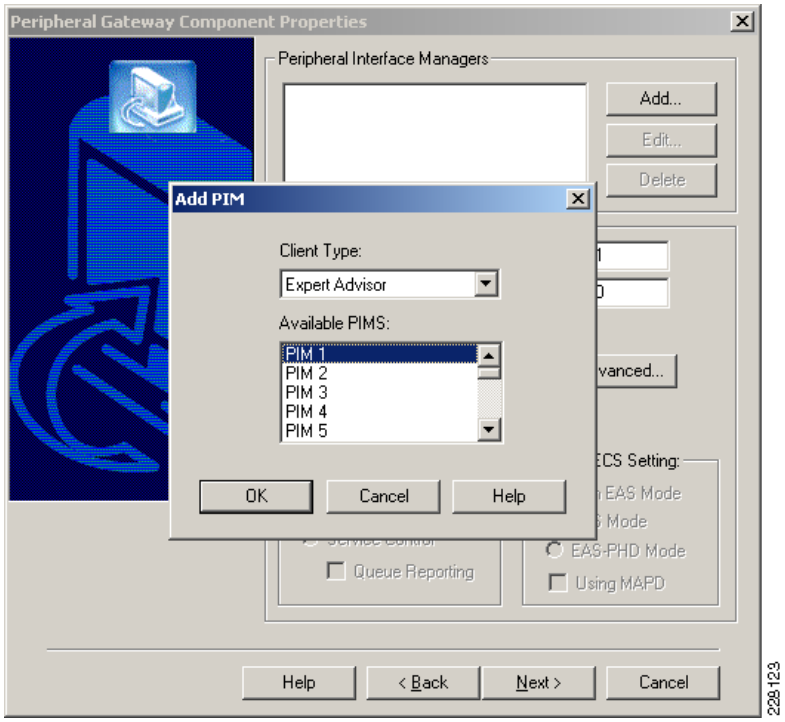
Figure B-51



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.

Note 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



Step 13 In the PIM Configuration dialogue, configure the PIM as follows:

a. Select **Enable**.

b. Enter an appropriate Peripheral name.

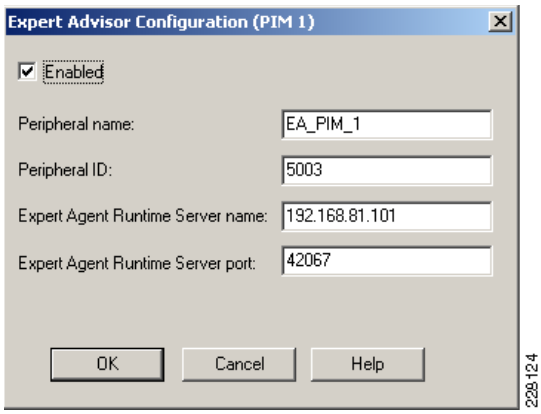
c. Enter the Peripheral ID that was assigned by the Configuration Manager on the Admin Workstation.

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.

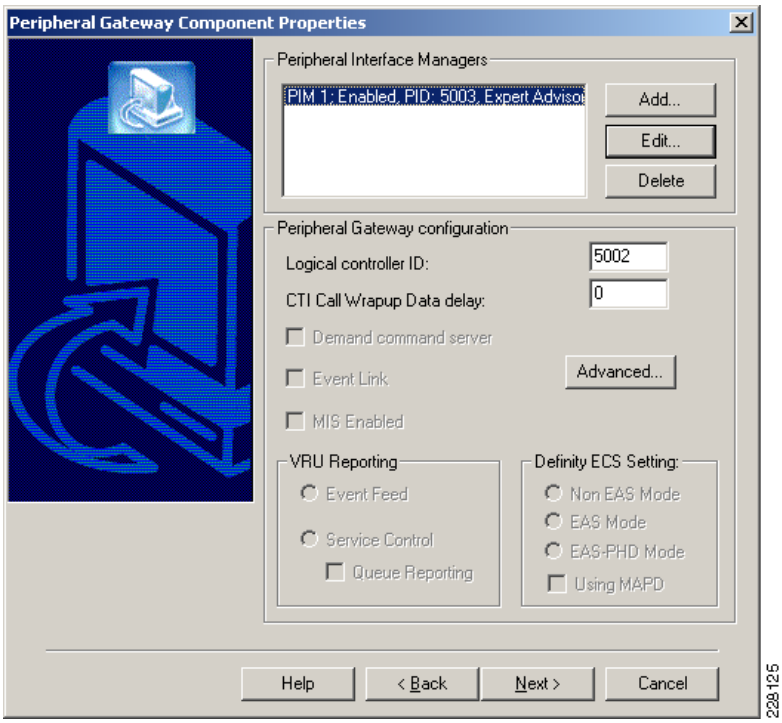
f. Click **OK**. See Figure B-53.

Figure B-53



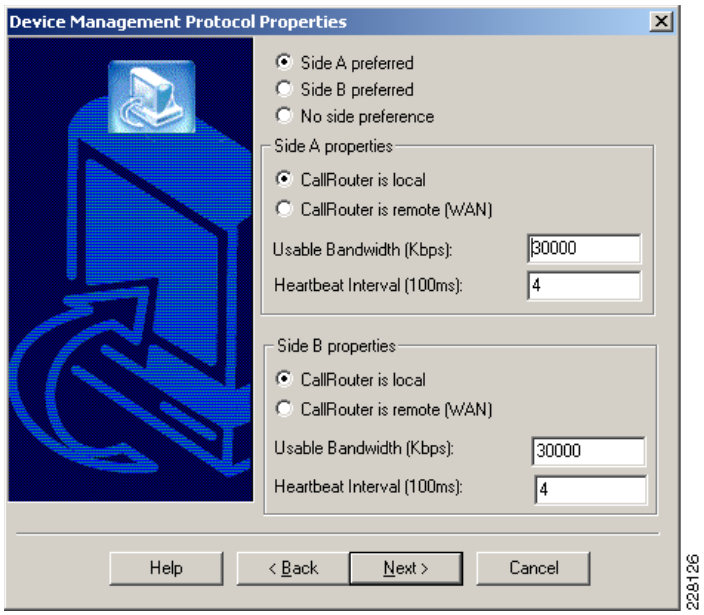
Back on the Peripheral Gateway Component Properties, enter the Peripheral Gateway Logical controller ID that was generated for the Expert Advisor PG by the Configuration Manager on the Admin Workstation and then click **Next**. See Figure B-54.

Figure B-54



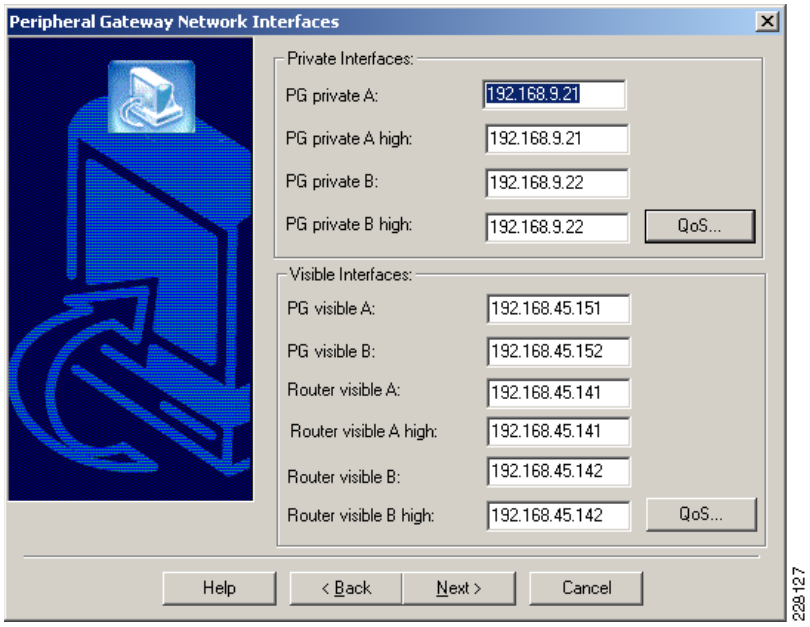
Step 14 On the Device Management Protocol Properties set **Side A preferred** option and click **Next**. See Figure B-55.

Figure B-55



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



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.

Figure B-57

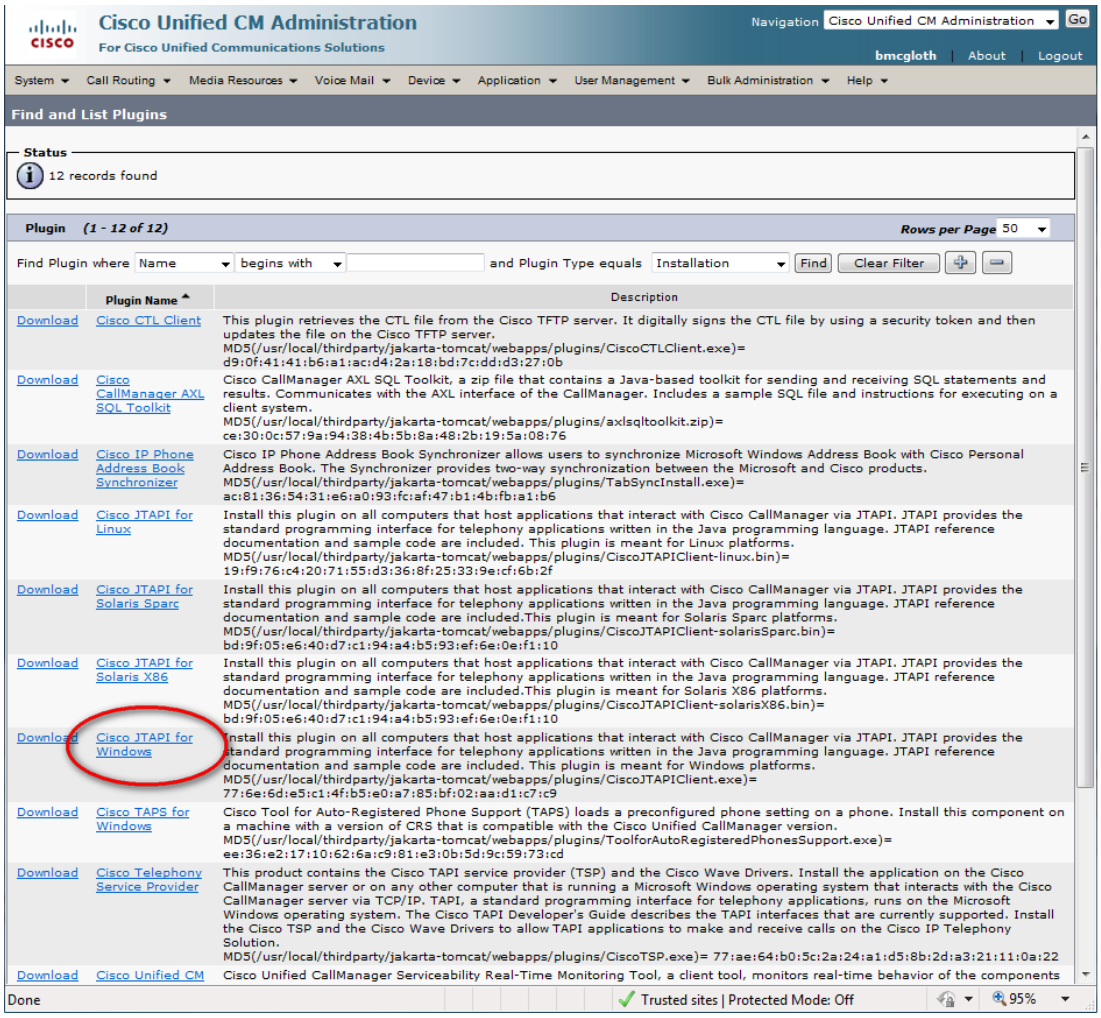
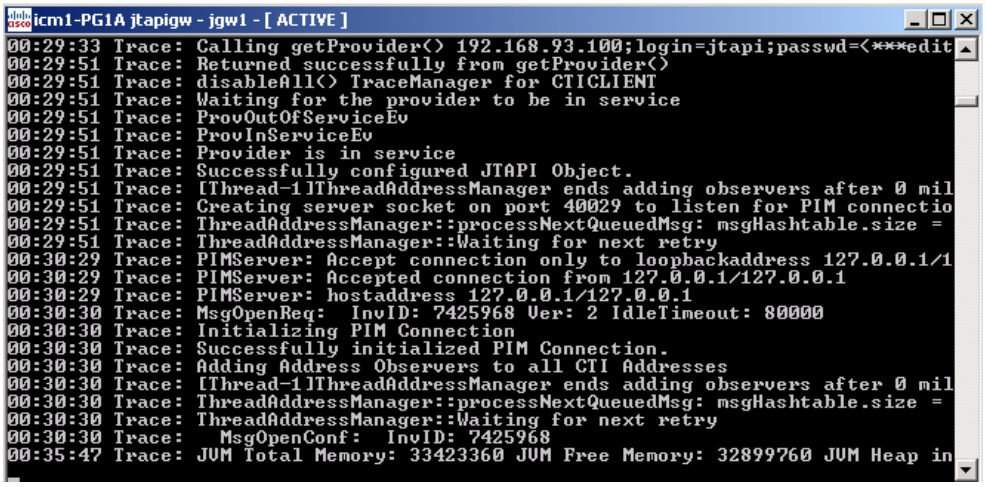


Figure B-58



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

CTI Server Installation

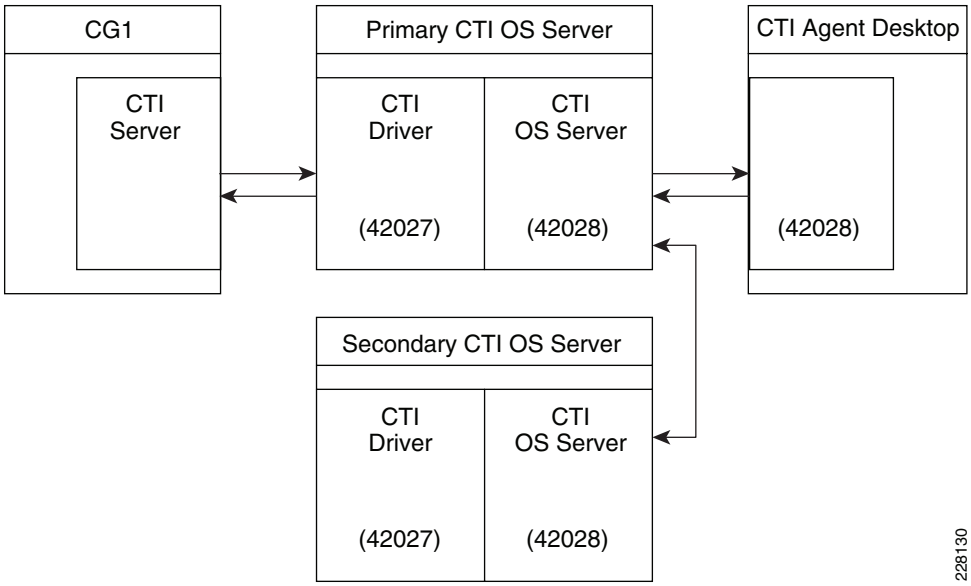
The CTI Server is an optional ICM node that allows a desktop or server application to receive call control information from the ICM and from call center peripherals. This information can be used, for example, in a screen pop on the agent's desktop. The CTI Gateway is available as part of the Cisco Enterprise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

Note 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.

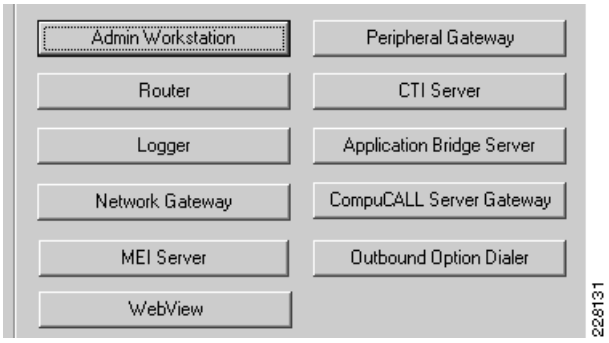
CTI Server (*ctisvr*) is also called CG (short for CTI Gateway) which connects to the CTI OS Server using the *ctidriver* service running on the CTI OS Server machine. Logically, it can be viewed as shown in Figure B-59.

Figure B-59 CTI Communication



In the ICM Setup application, click the **Add** button on the right under **Instance Components**. See Figure B-60.

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**.

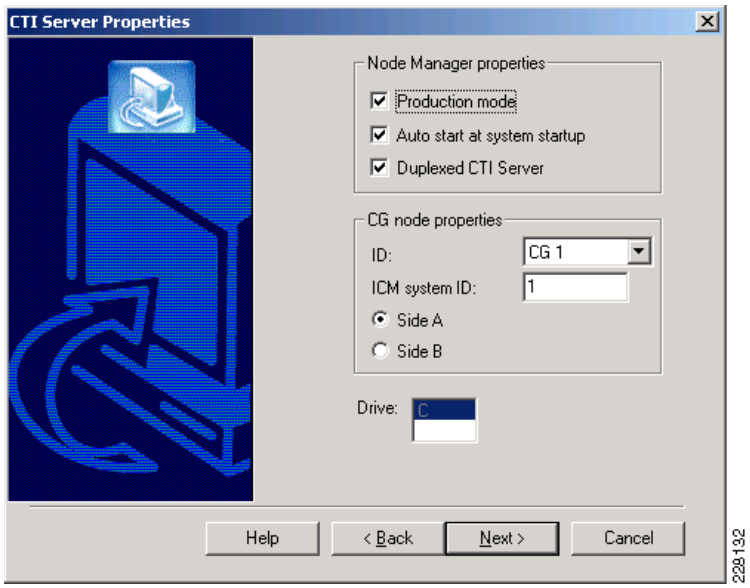
Step 2 Check the **Auto start at system startup**.

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.

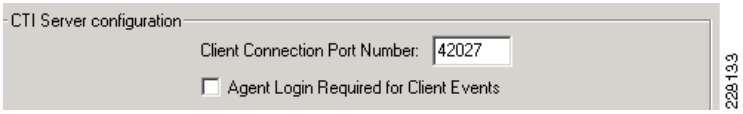
Step 5 Click **Next**. See Figure B-61.

Figure B-61



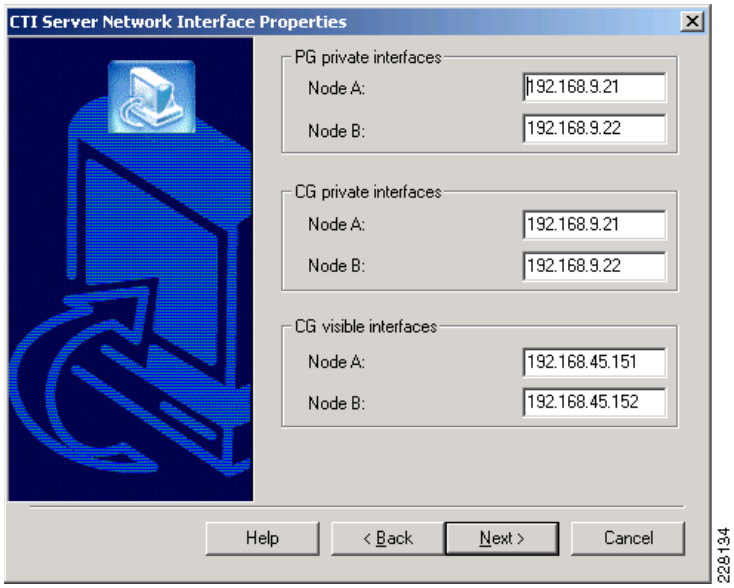
Step 6 CTI Server as a default connects to the CTIOS Server on port 42027, but can be configured to use a different port. Click **Next**. See Figure B-62.

Figure B-62



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

Figure B-63



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.

Figure B-64

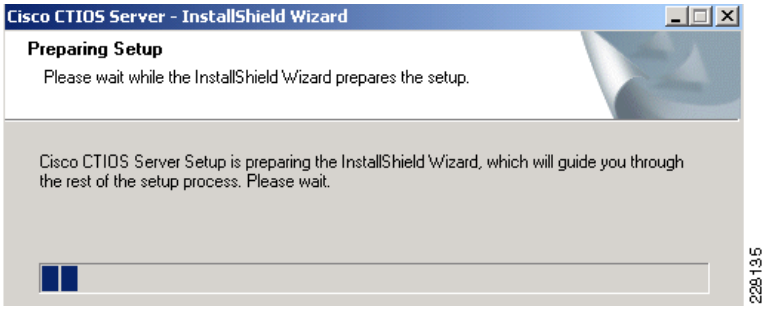
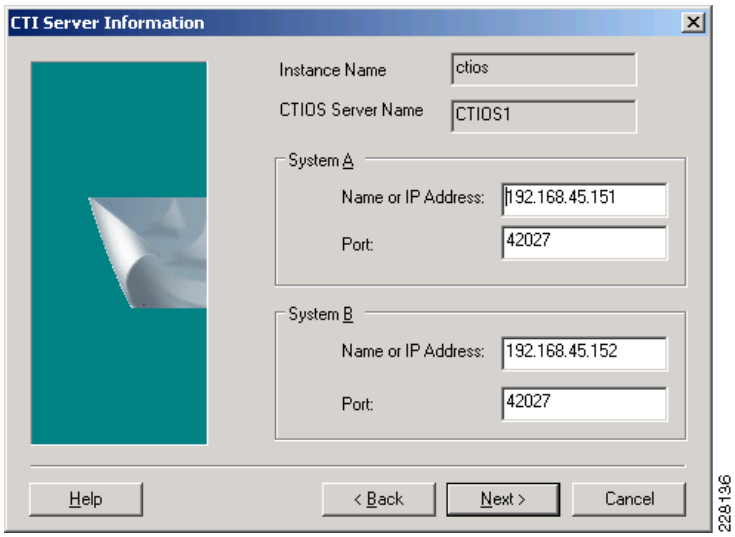
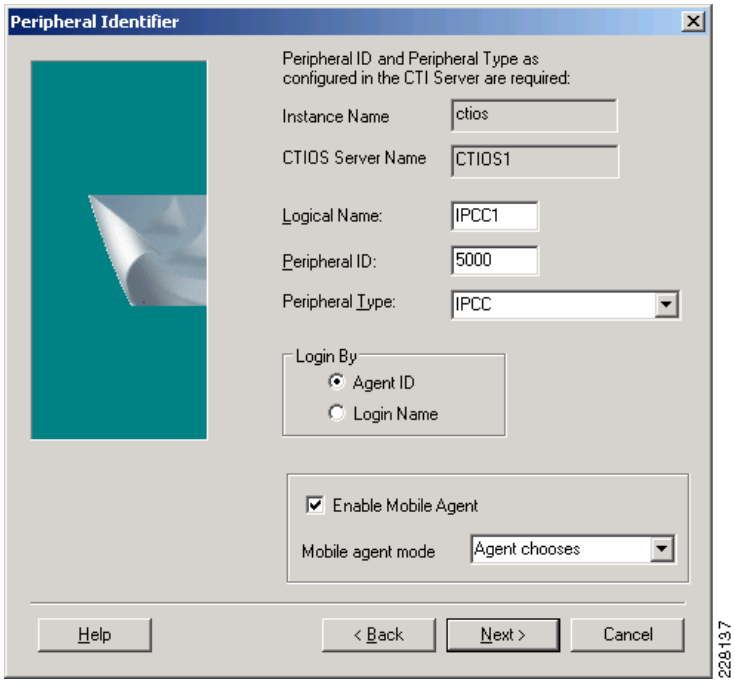


Figure B-65



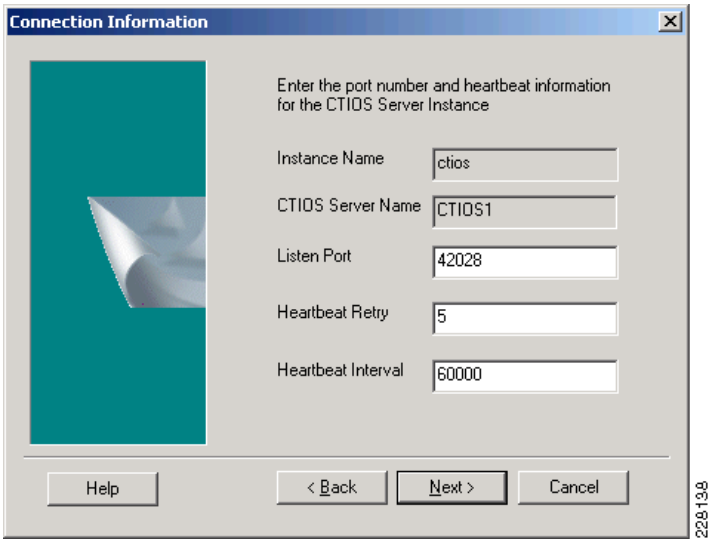
Step 5 The Peripheral ID here is the same ID that was assigned during the CUCM PG configuration in the Configuration Manager on AW. The agent desktop communicates with the CUCM IP Phone. See Figure B-66.

Figure B-66



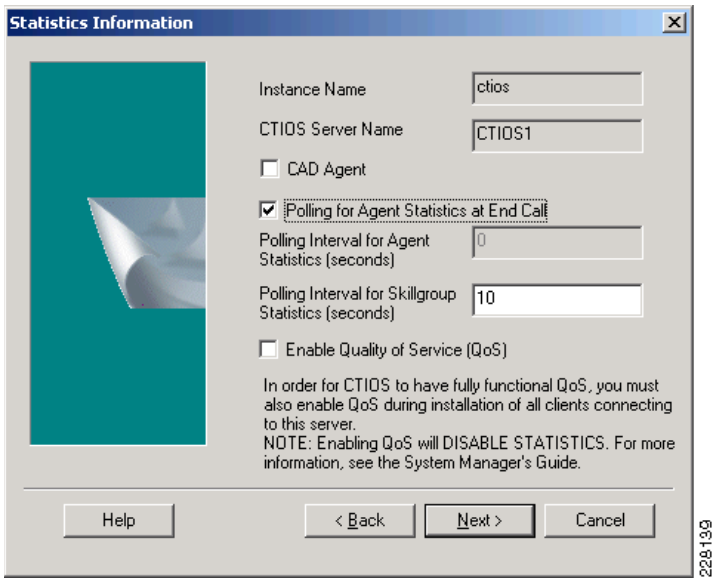
Step 6 The listen port is where CTI Desktop Agent will connect. This port will also be used if a secondary CTIOS Server wants to talk to this one in an high availability environment or setting. See Figure B-67.

Figure B-67



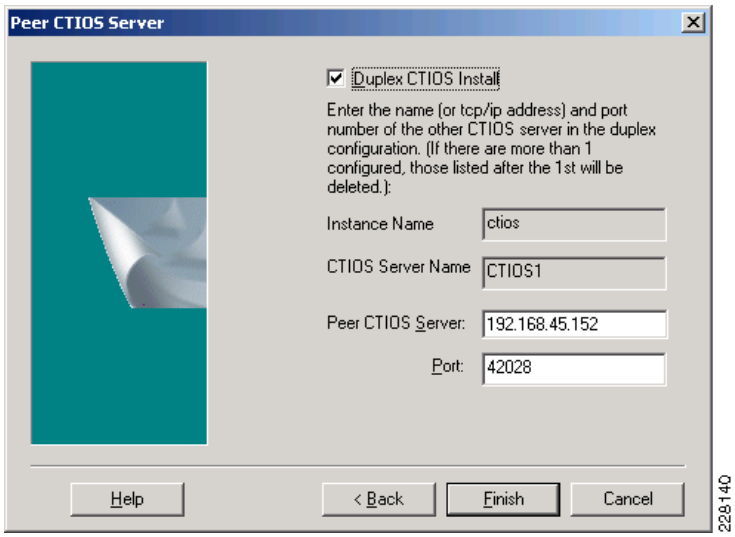
Step 7 Enter the default polling interval for Skillgroup statistics (in seconds). Click **Next**. See Figure B-68.

Figure B-68



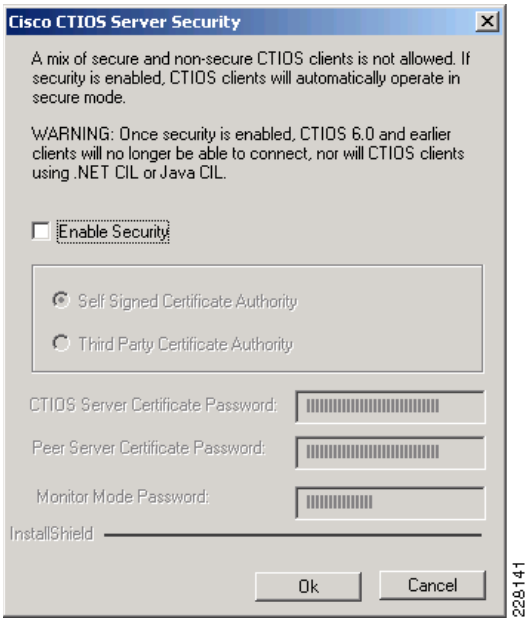
Step 8 The Peer CTIOS Server dialog is used to configure a CTI OS Peer Server. It is also used for Chat and CTI OS Silent Monitoring. Enter the appropriate information. After you click **Finish**, and the files are laid down, the service is registered, and Registry entries are made. See Figure B-69.

Figure B-69



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

Figure B-70



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”.

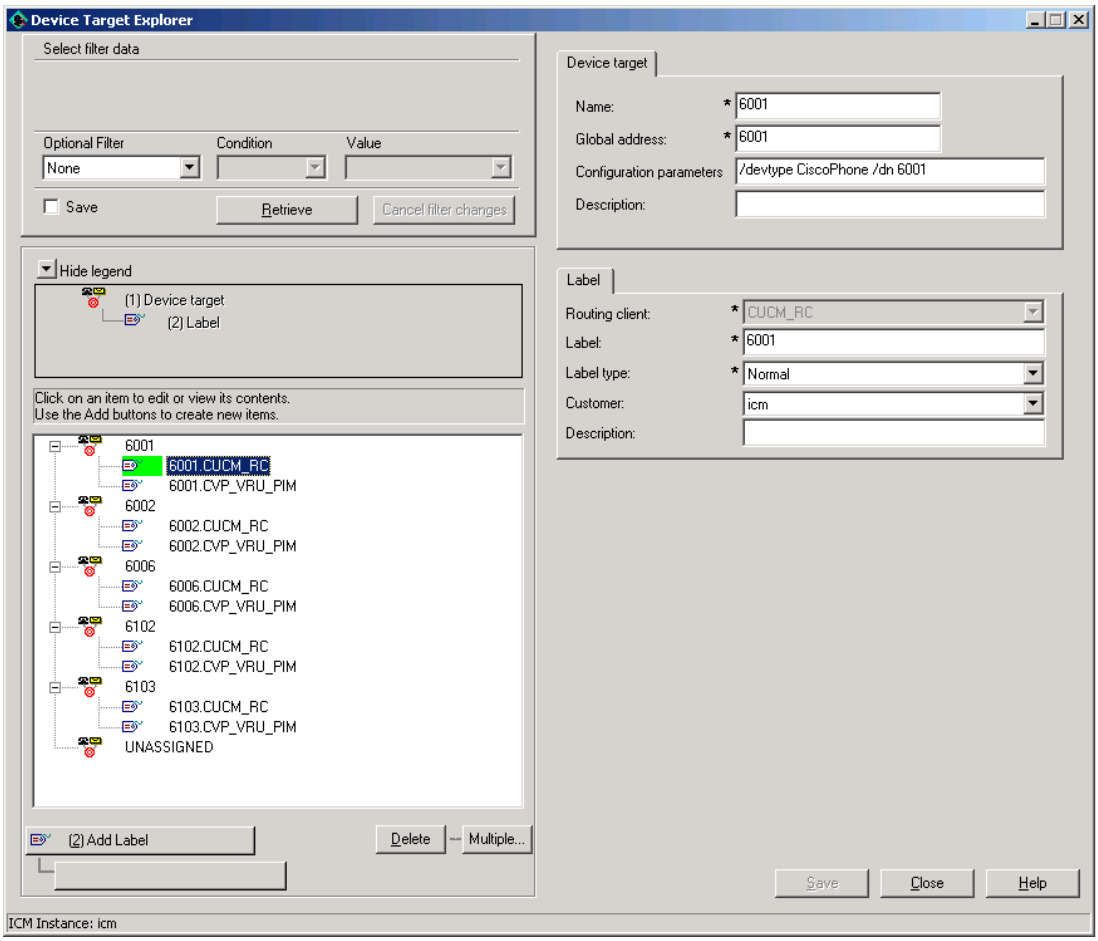
Step 6 Enter the Global Address, also the extension number for fully qualified number.

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.

Figure B-71



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.

Figure B-72

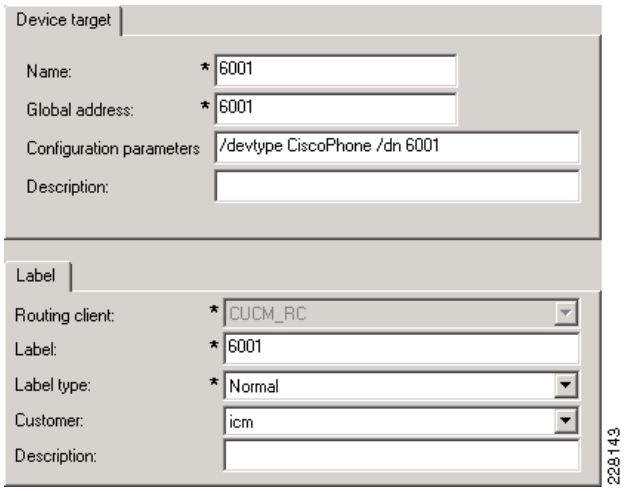
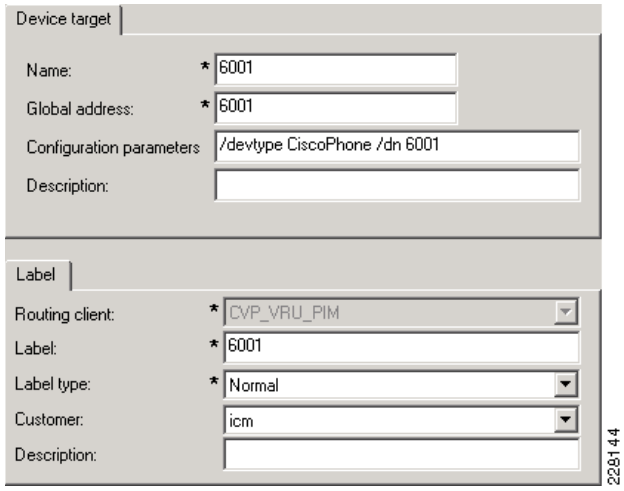


Figure B-73 shows a label defined for CVP Routing Client.

Figure B-73



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**.

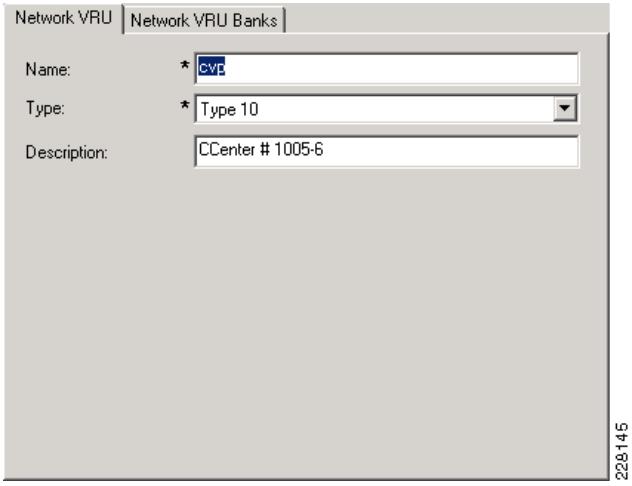
Step 5 Enter an appropriate name such as "**cvp**".

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



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**.

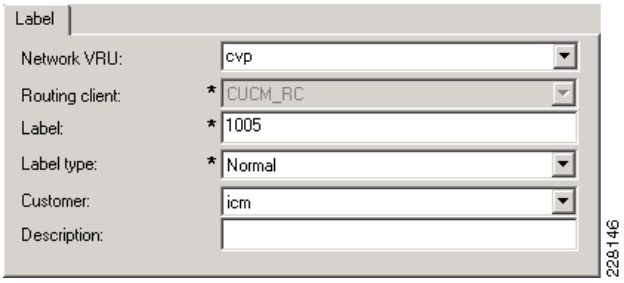
Step 5 Select **normal** for the label type.

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



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

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**.

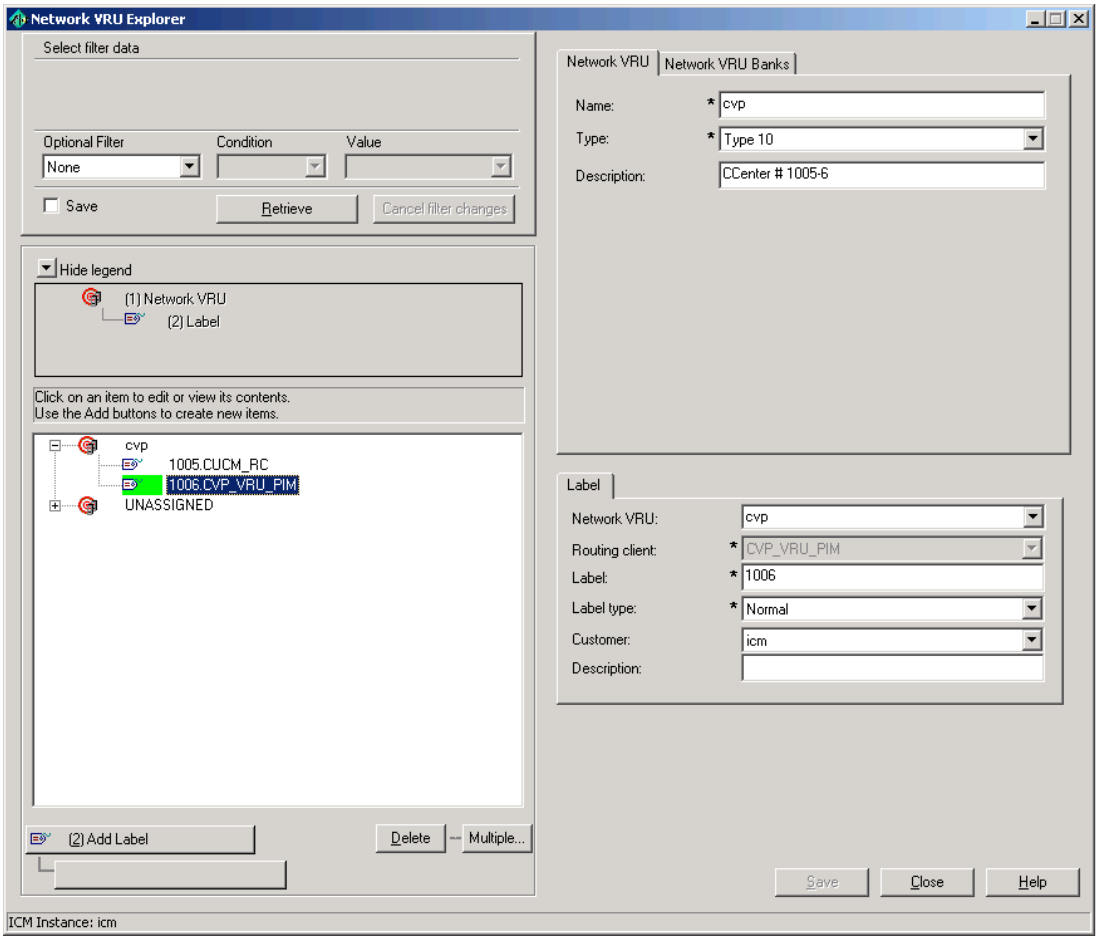
Step 5 Select **normal** for the label type.

Step 6 Select **icm** as the Customer.

Step 7 Enter a description as desired.

Step 8 Click **Save**. See Figure B-76.

Figure B-76



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.

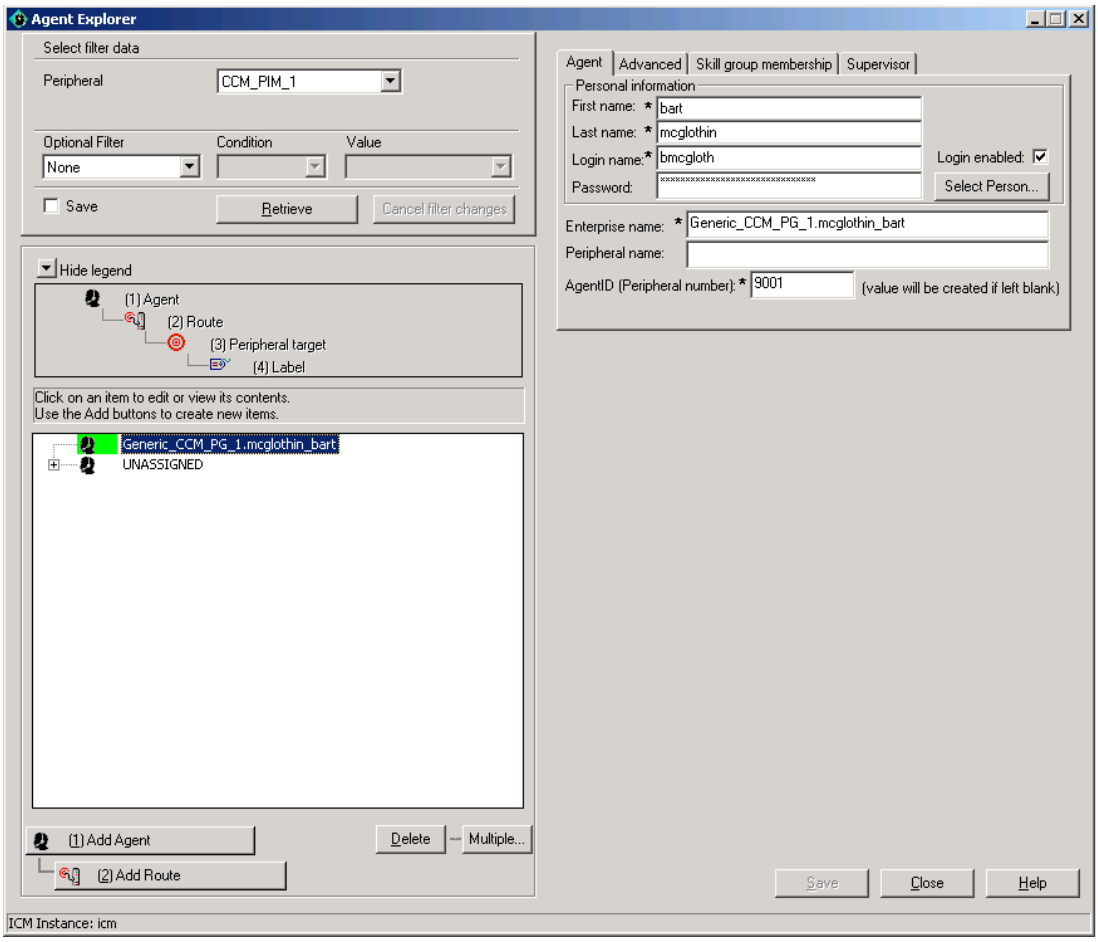
Step 7 Verity the Enterprise name that was generated is appropriate.

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.

Figure B-77



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**.

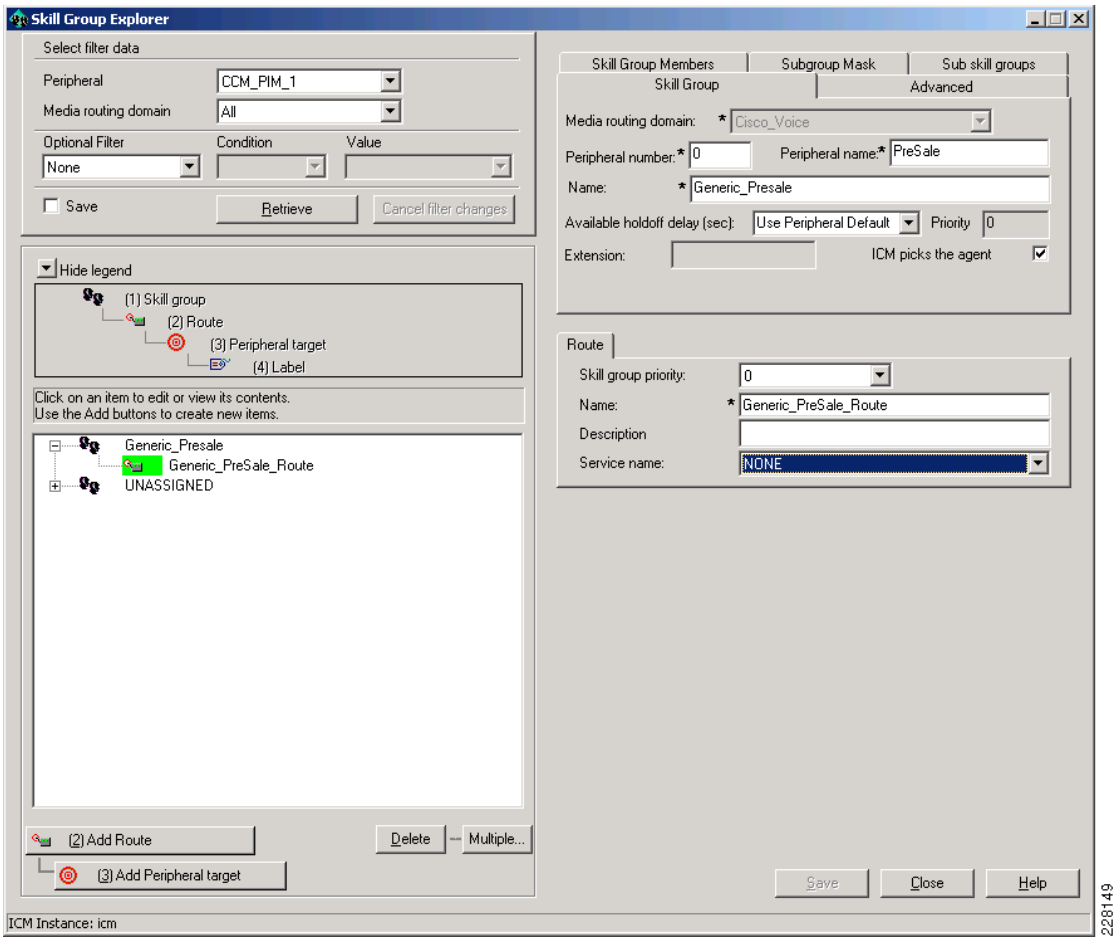
Step 10 Add route option in the skill group.

Step 11 Click **Add Route**.

Step 12 Assign an appropriate name such as **Generic_PreSale_Route**.

Step 13 Click **Save**. See Figure B-78.

Figure B-78



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**.

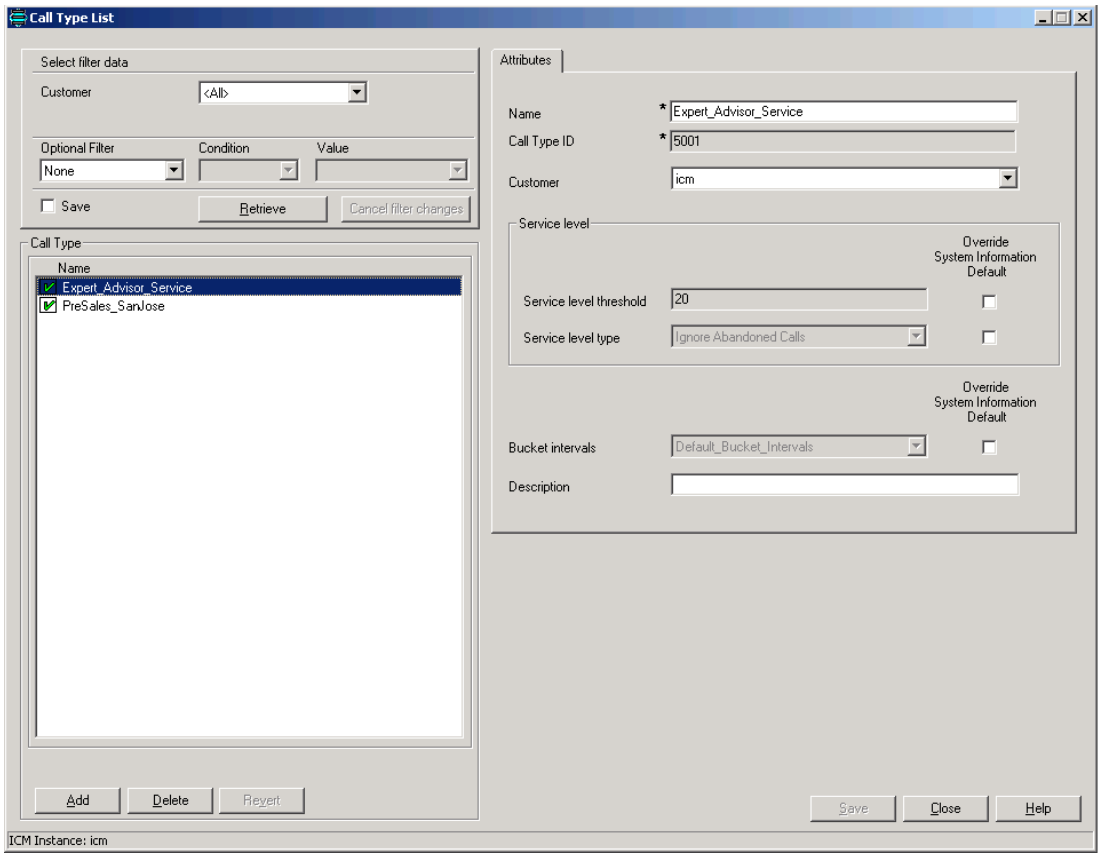
Step 6 Select the Customer **icm**.

Step 7 Enter an appropriate description as desired.

Step 8 Click **Save**. See Figure B-79.

Step 9 Repeat for second list.

Figure B-79



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**.

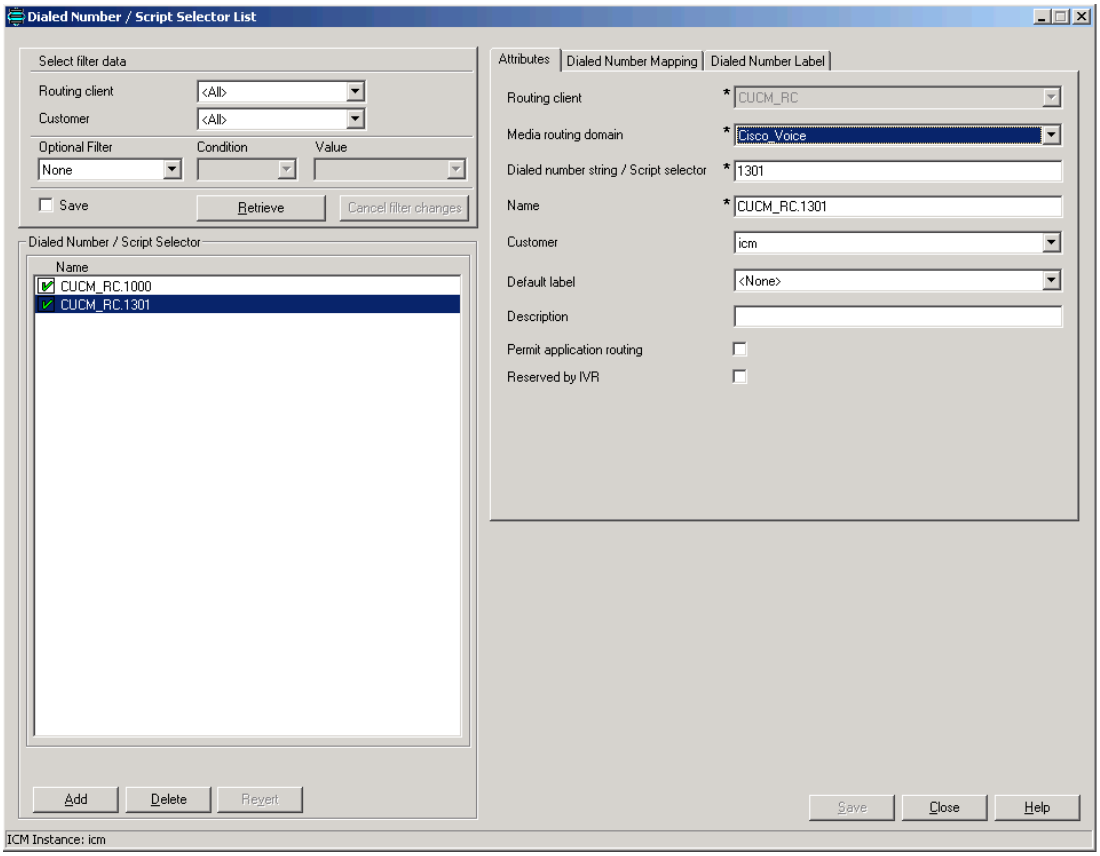
Step 10 Leave the default Label as **<None>**.

Step 11 Enter an appropriate description as desired.

Step 12 Click **Save**. See Figure B-80.

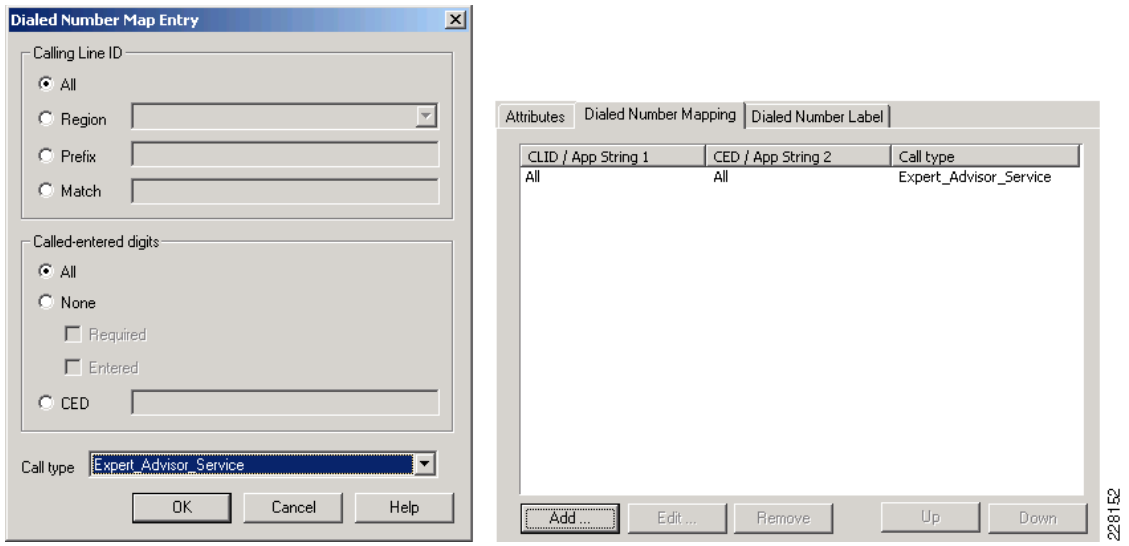
Step 13 Repeat for additional dialed numbers.

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.

Figure B-81



Enable Expanded Call Context

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

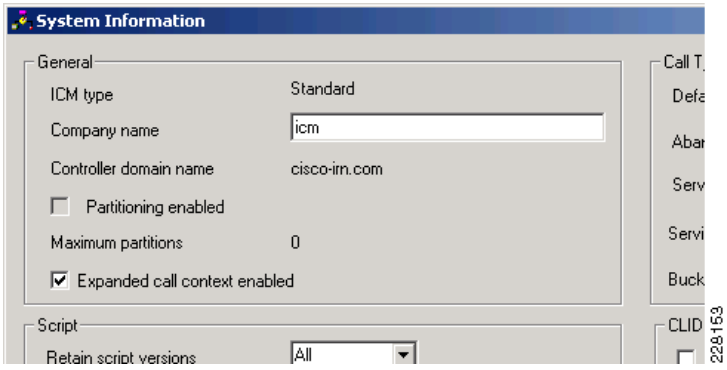
Step 1 Open the Configurations Manager on the AW.

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.

Figure B-82



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**.

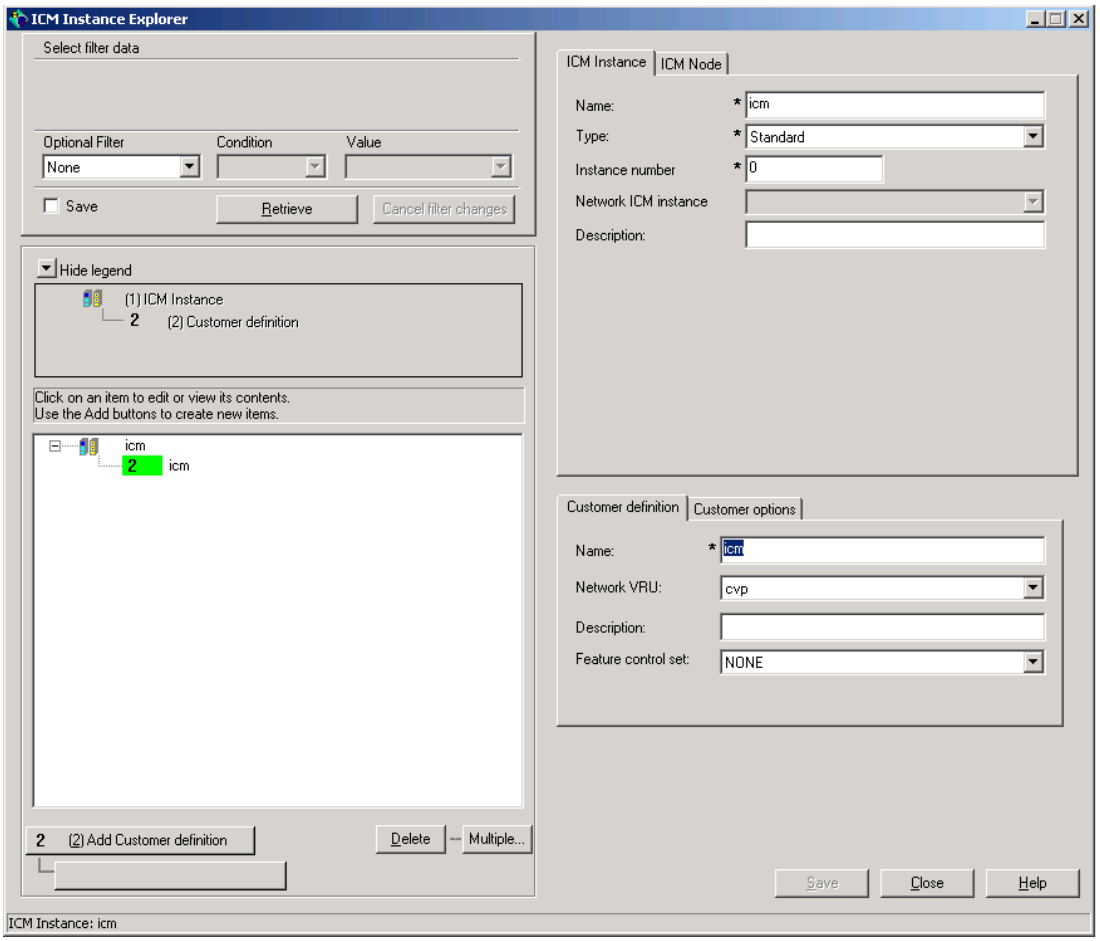
Step 6 Enter an appropriate name.

Step 7 Select the Network VRU as **cvp**.

Step 8 Enter an appropriate description as desired.

Step 9 Click **Save**. See Figure B-83.

Figure B-83



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.

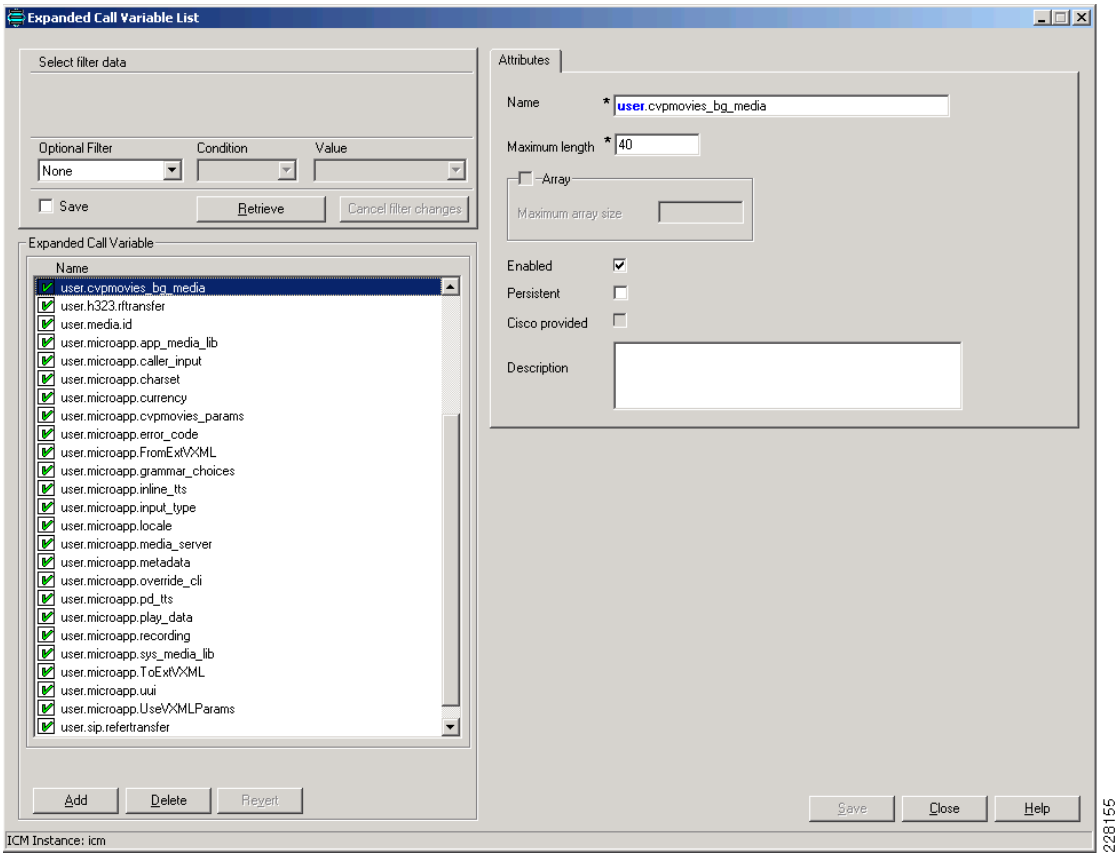
Table B-1 Expanded Call Variables

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)

user.microapp.override_cli	1		Yes	
user.microapp.pd_tts	1		Yes	
user.microapp.play_data	40		Yes	
user.microapp.recording	40		Yes	
user.microapp.sys_media_lib	10		Yes	
user.microapp.ToExtVXML	210	1	Yes	
user.microapp.uui	131		Yes	
user.microapp.UseVXMLParams	1	1	Yes	
user.sip.refertransfer	1		Yes	
user.video_media_server	40		Yes	

Figure B-84



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.

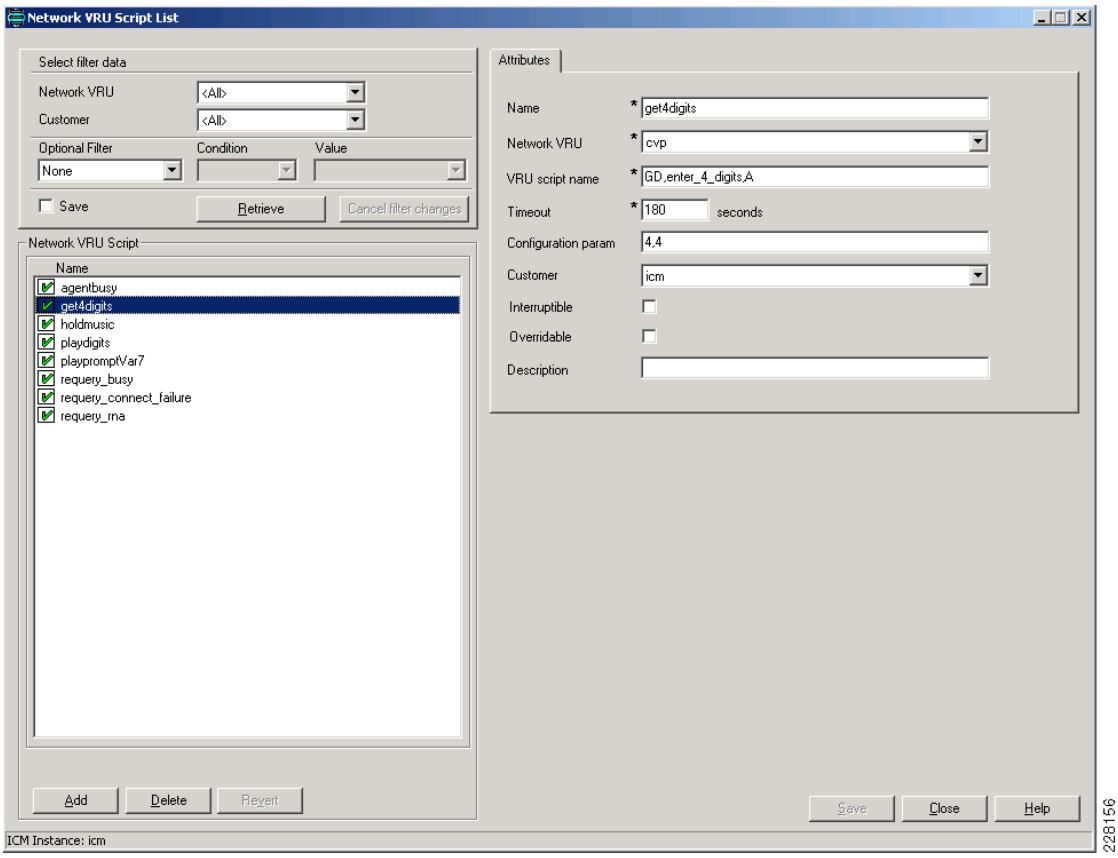
Step 13 Click **Save**.See Figure B-85.

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		y	Y
playdigits	PD,Char	180		y	
playpromptVar7	PM,-7	180		y	
requery_busy	PM,requery_busy	180			
requery_connect_failure	PM,requery_connect_failure	180			
requery_rna	PM,requery_rna	180			

Figure B-85



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 Not*e 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.

Figure B-86

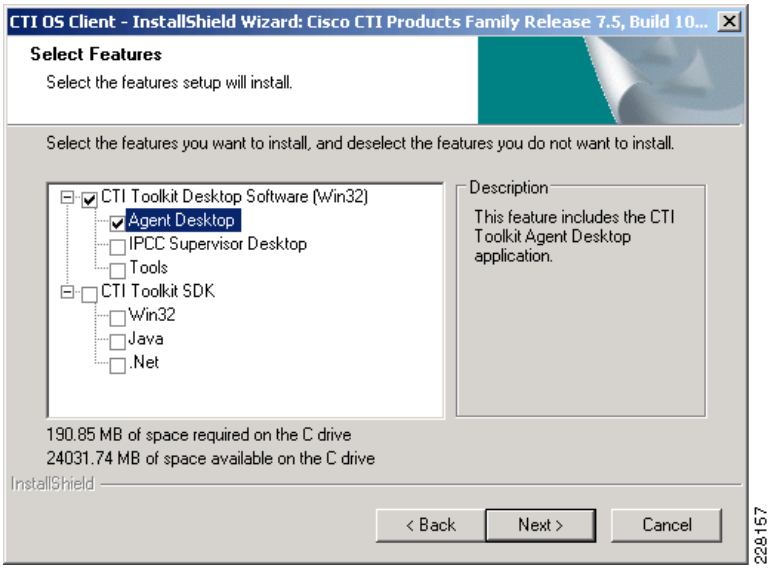
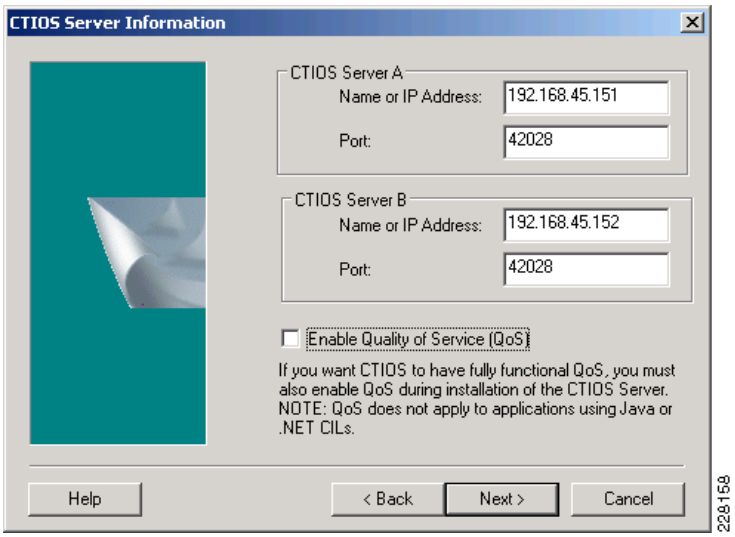


Figure B-87



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 *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 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 *Call.user.microapp.play_data* variable.

Step 9 Run another external scrip called *playdigits*. This script will play the value stored in *Call.user.microapp.play_data* variable.

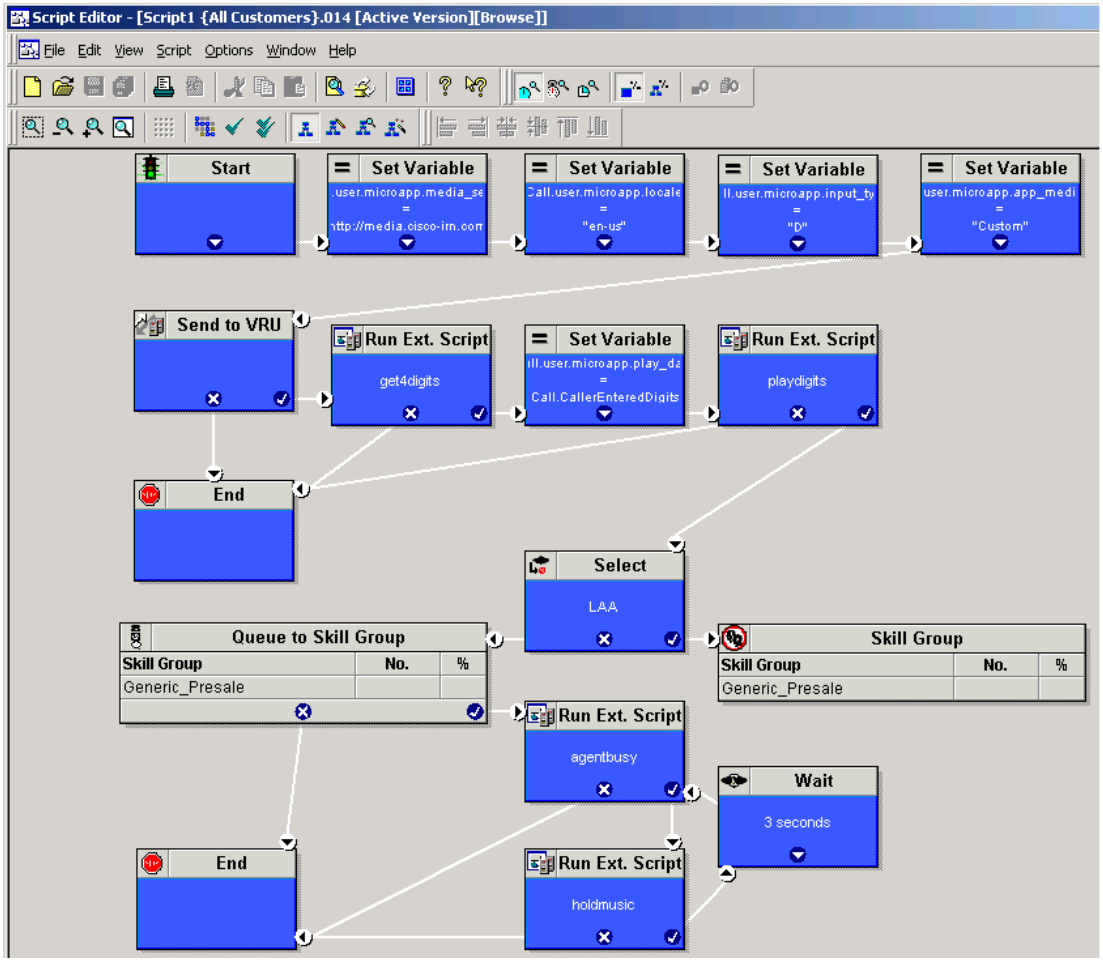
Step 10 The select Longest Available Agent (LAA) decision object.

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.

Figure B-88



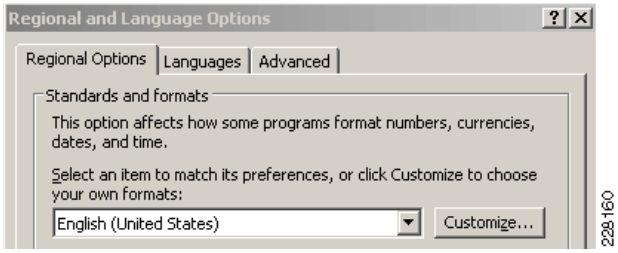
Cisco Voice Portal Installation

Prerequisites

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

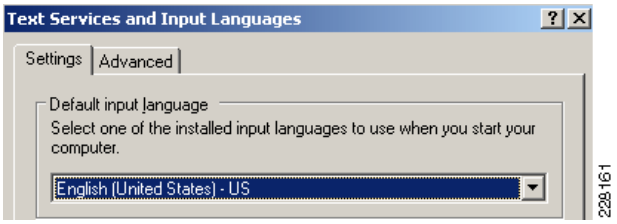
See Figure B-89.

Figure B-89



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

Figure B-90



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

Figure B-91

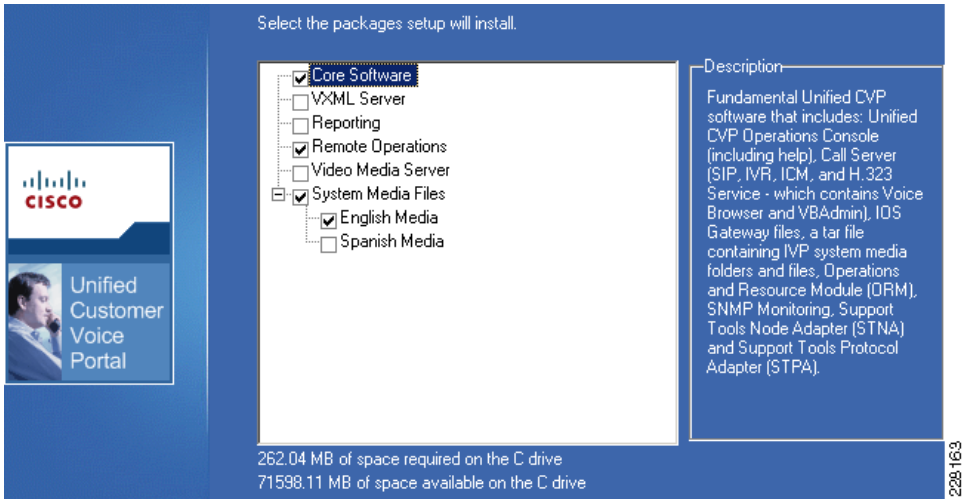
CVP Call Server, Operation Console and Media Server Installation

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:

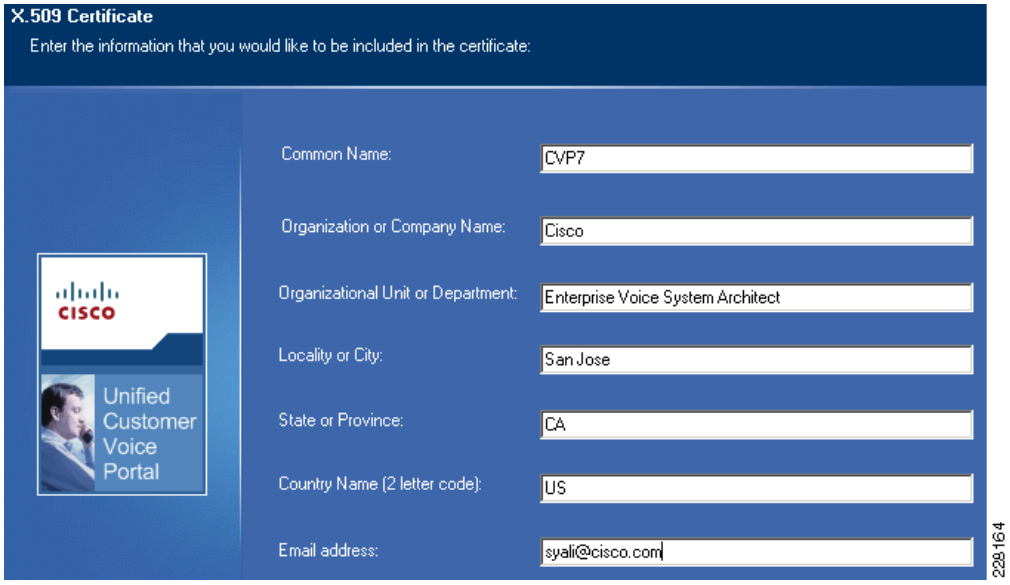
Step 1 Select Core Software, Remote Operations and System Media Files. See Figure B-92.

Figure B-92



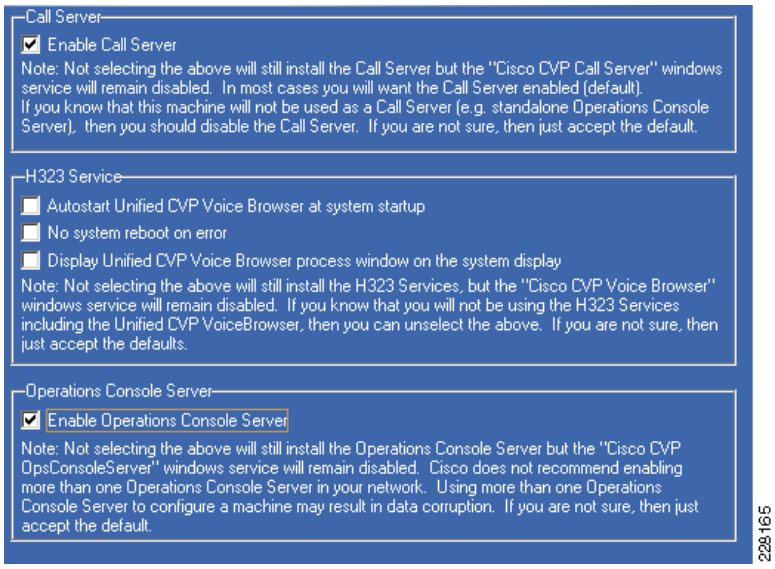
Step 2 Enter appropriate security certificate information. See Figure B-93.

Figure B-93



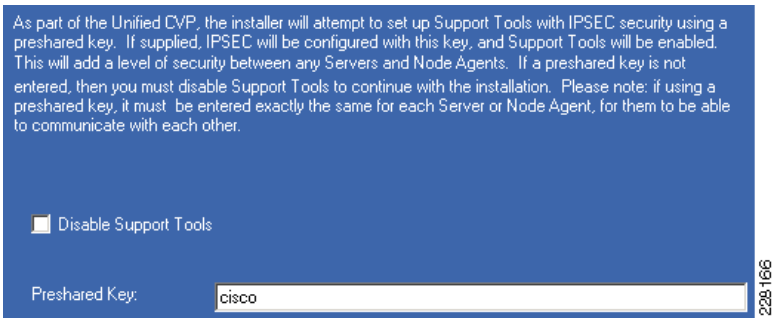
Step 3 Enable the Call server and the Operations console.See Figure B-94.

Figure B-94



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

Figure B-95



CVP Component Configuration

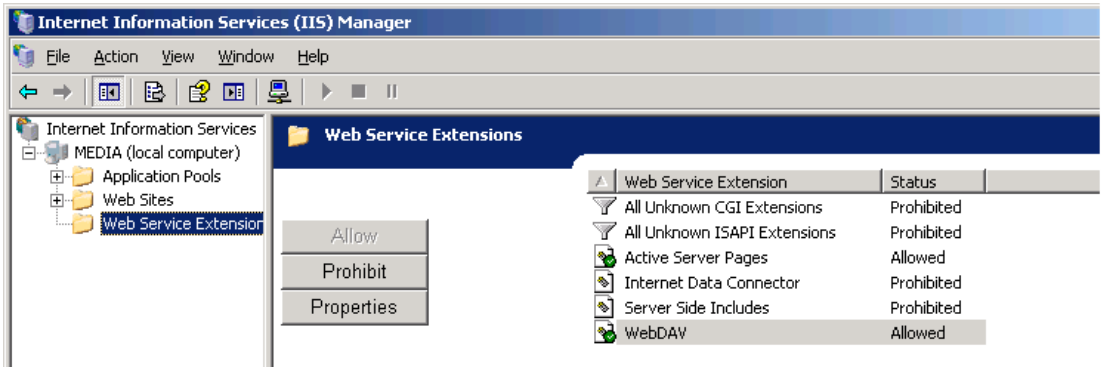
There are several components that needs to be configured before CVP can operate properly. They are as follows:

- CVP Media Server Configuration
- CVP Call Server Configuration

CVP Media Server Configuration

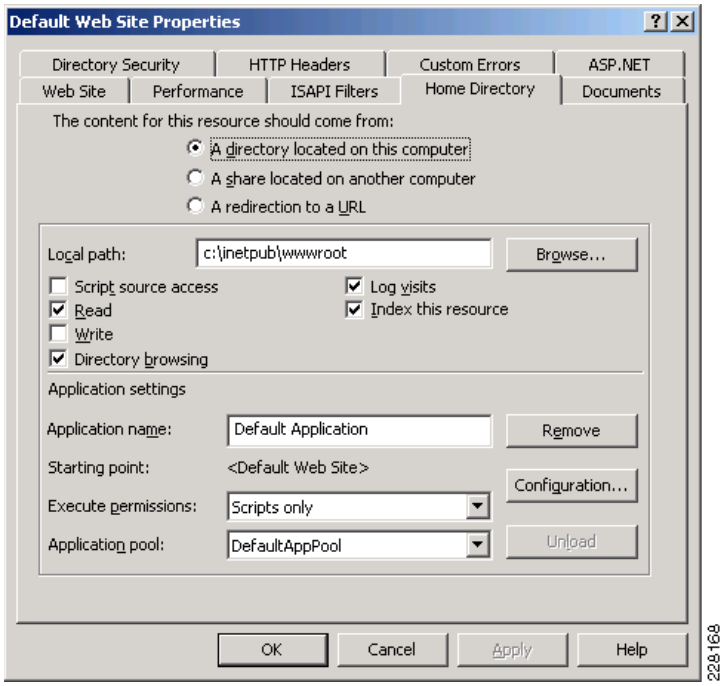
This setup used Microsoft IIS as the web server to host the media files. See Figure B-96.

Figure B-96



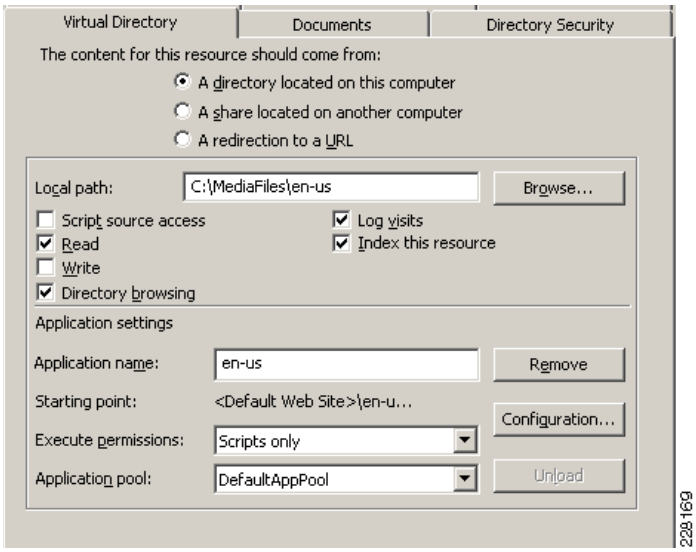
Step 1 Enable read permission to the directory where **.wav** files are saved. See Figure B-97.

Figure B-97



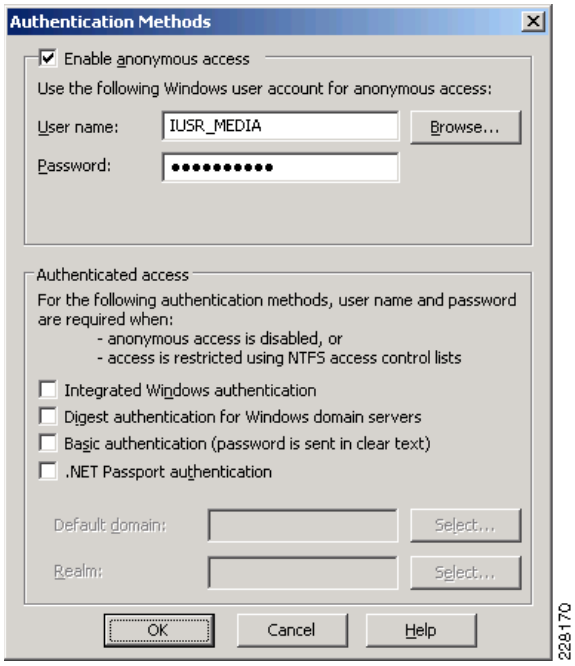
Step 2 Either create a Virtual Directory linking to the Media Files installed by the CVP **setup.exe**, or copy the "**en-us**" folder to the root of the IIS Web server. See Figure B-98.

Figure B-98



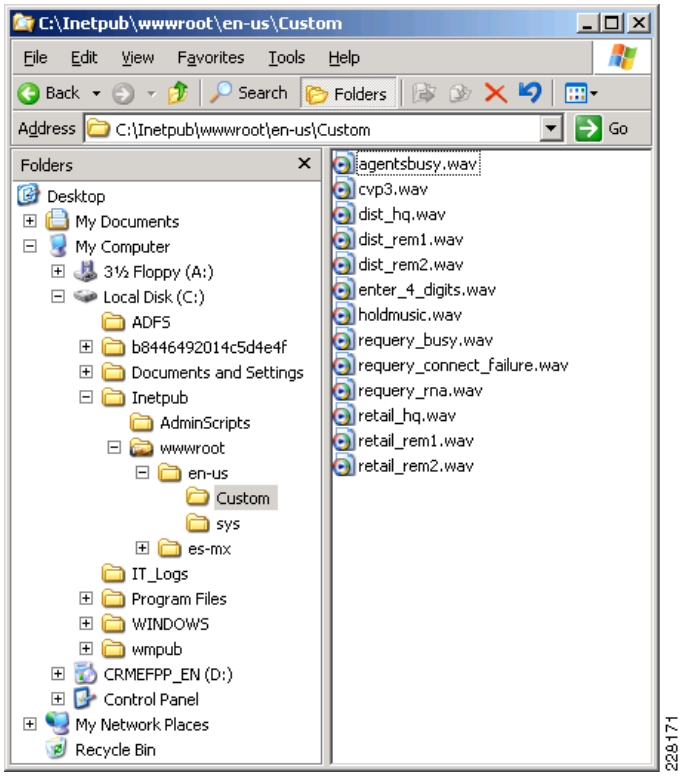
Step 3 Make sure anonymous access is enabled and the built-in IIS User is assigned. See Figure B-99.

Figure B-99



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

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

Table B-3 CUCM Originated Calls (continued)

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

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

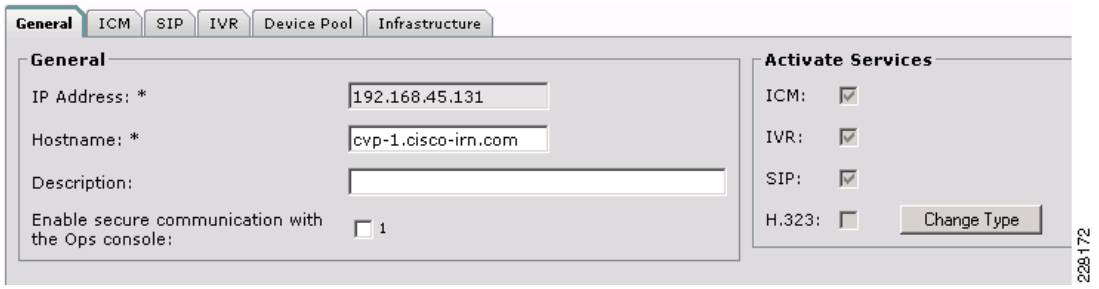
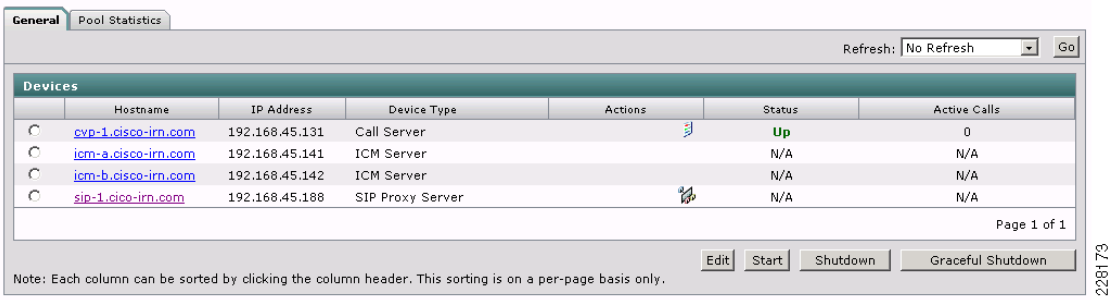


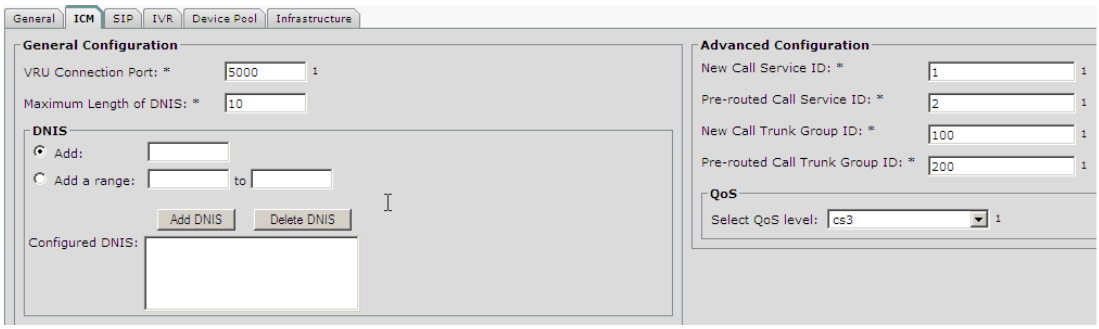
Figure B-102



CVP Call Server ICM Configuration

See Figure B-103.

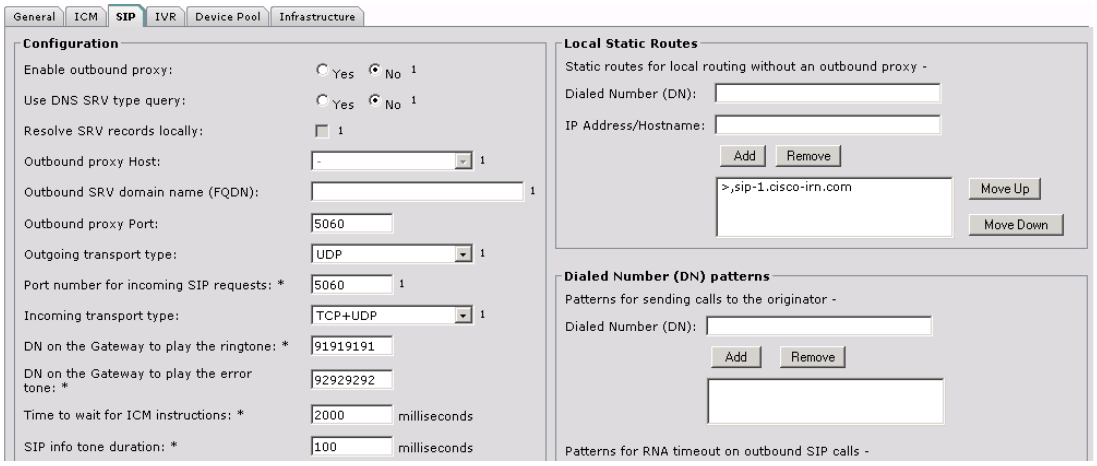
Figure B-103



CVP Call Server SIP Configuration and Static Route

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

Figure B-104



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
!
hostname VXML
!
boot-start-marker
boot system flash c2800nm-ipvoicek9-mz.124-24.T1.bin
boot-end-marker
!
logging message-counter syslog
logging buffered 100000
enable password cisco
!
no aaa new-model
clock timezone PST -8
clock summer-time PSTDST recurring
!
dot11 syslog
ip source-route
!
!
ip cef
!
!
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
!
!
!
voice class codec 1
 codec preference 1 g711ulaw
 codec preference 2 g729r8
!
voice class h323 1
  h225 timeout setup 3
!
!
voice translation-rule 1
 rule 1 /987654/ //
!
!
voice translation-profile block
 translate called 1
!
!
voice-card 0
 dsp services dspfarm
!
http client cache memory pool 15000
http client cache memory file 500
ivr prompt memory 15000
!
application
 service new-call flash:bootstrap.vxml
  paramspace english language en
  paramspace english index 0
  paramspace english location flash:
  paramspace english prefix en
 !
 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
 !
 service ringtone flash:ringtone.tcl
  paramspace english language en
  paramspace english index 0
  paramspace english location flash
  paramspace english prefix en
 !
 service recovery flash:recovery.vxml
  paramspace english language en
  paramspace english index 0
  paramspace english location flash:
  paramspace english prefix en
 !
 service cvperror flash:cvperror.tcl
  paramspace english index 0
  paramspace english language en
  paramspace english location flash
  paramspace english prefix en
 !
 service takeback flash:survivability.tcl
  paramspace english language en
  paramspace english index 0
```

```
  paramspace english location flash
  paramspace english prefix en
 !
 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
 !
 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
 !
!
vxml version 2.0
!
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
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet1/0
 no ip address
 shutdown
!
!
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
!
control-plane
!
mgcp fax t38 ecm
mgcp behavior g729-variants static-pt
!
! <====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
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate profile 1 register MTP-01
!
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
!
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 vad
!
dial-peer voice 9292 voip
 service cvperror
 session protocol sipv2
 incoming called-number 9292T
 dtmf-relay rtp-nte
 codec g711ulaw
 no vad
!
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
!
dial-peer voice 987654 voip
 translation-profile incoming block
 incoming called-number 987654
!
!
!
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

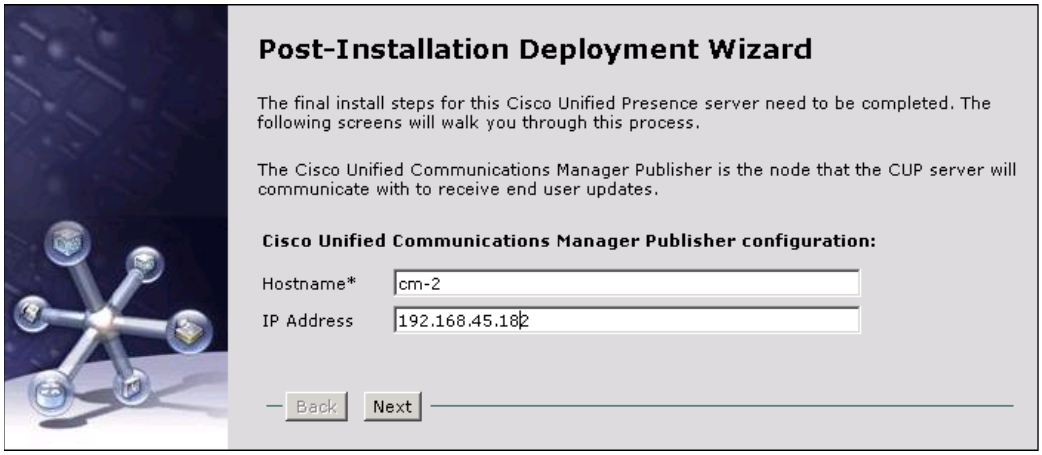


Figure B-106

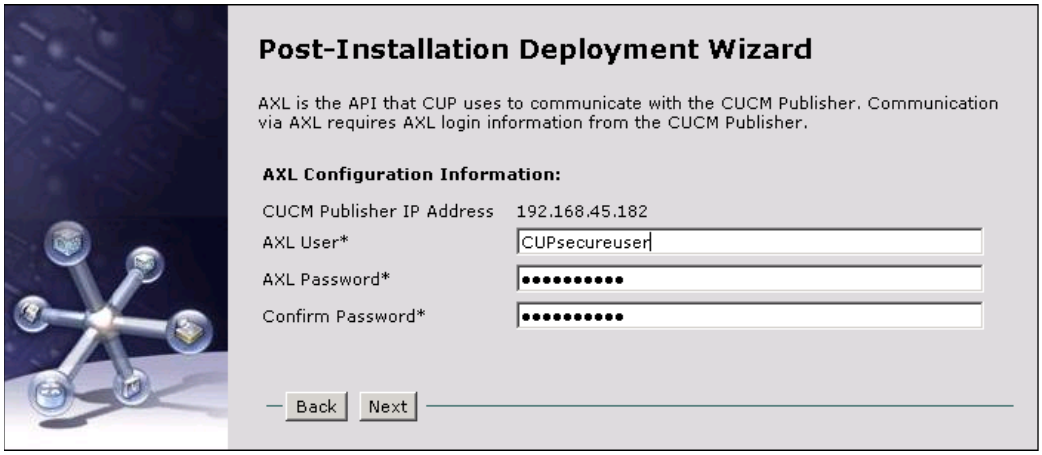
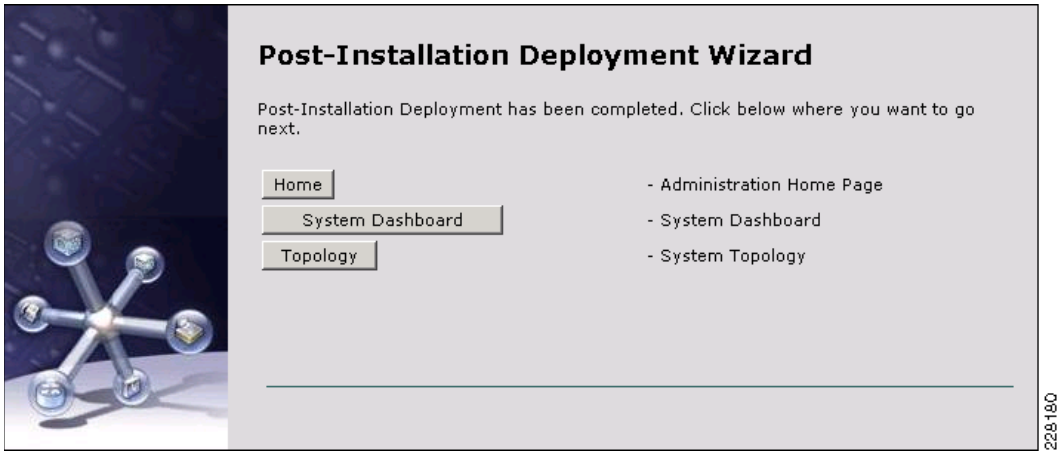


Figure B-107

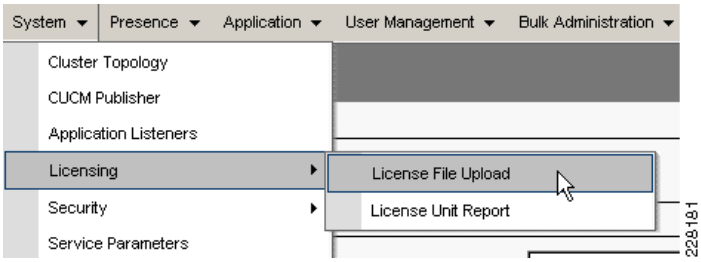
Figure B-108

Figure B-109



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

Figure B-110

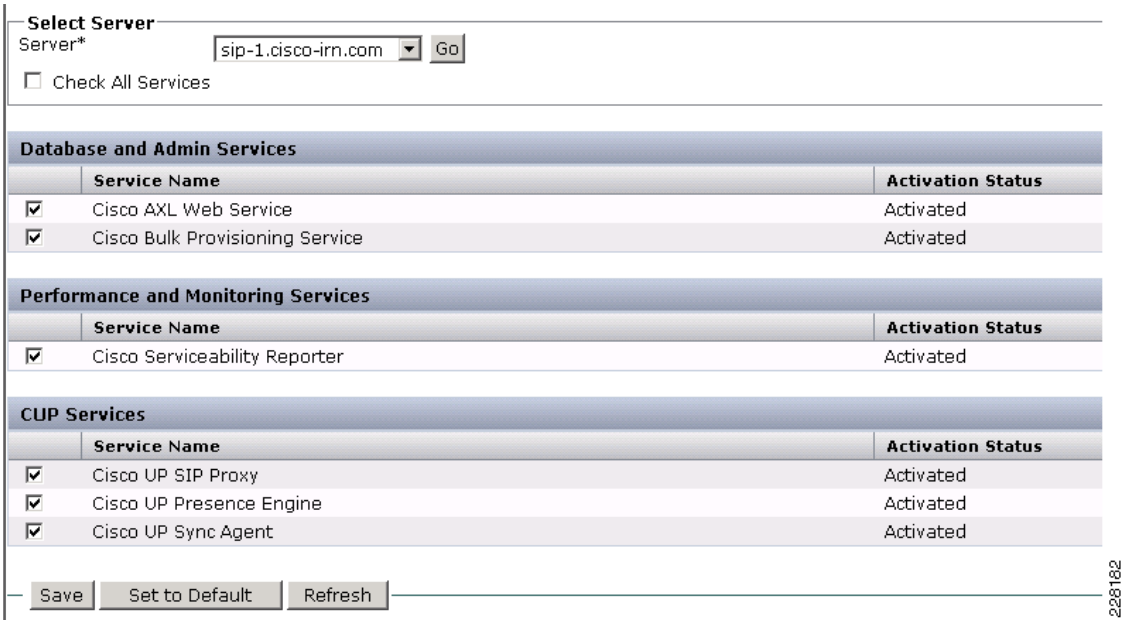


Configuration

CUP

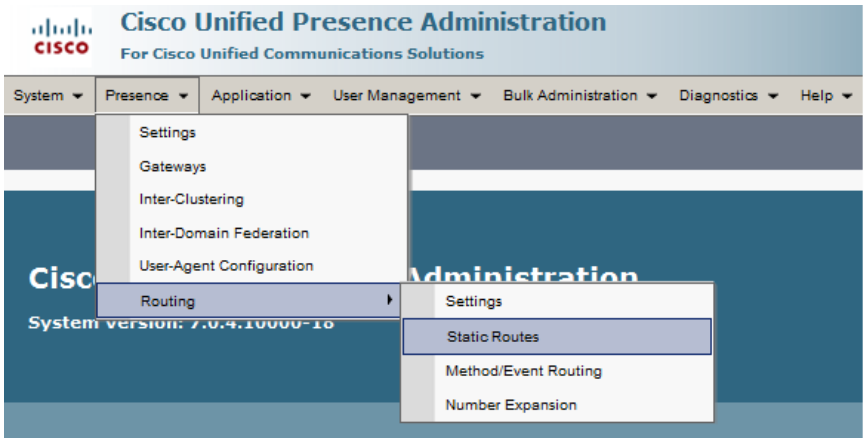
Step 1 Activate the **Cisco UP SIP Proxy**, **Cisco UP Presence and Cisco UP Sync Agent** Services. See Figure B-111.

Figure B-111



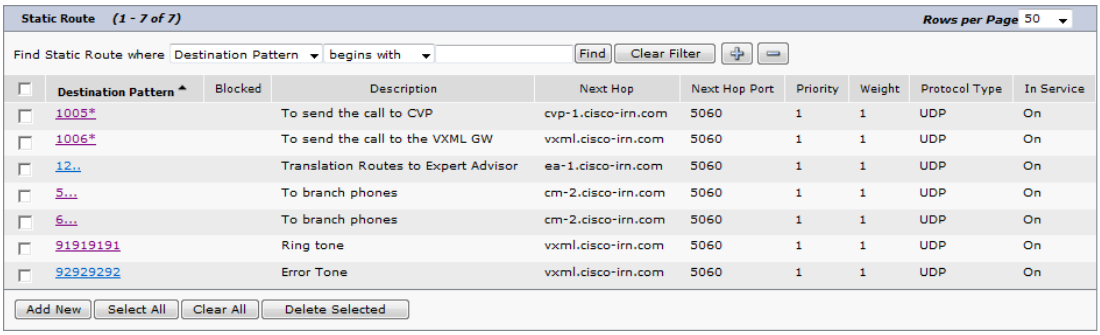
Step 2 Go to **Presence > Routing > Static Routes**. See Figure B-112.

Figure B-112



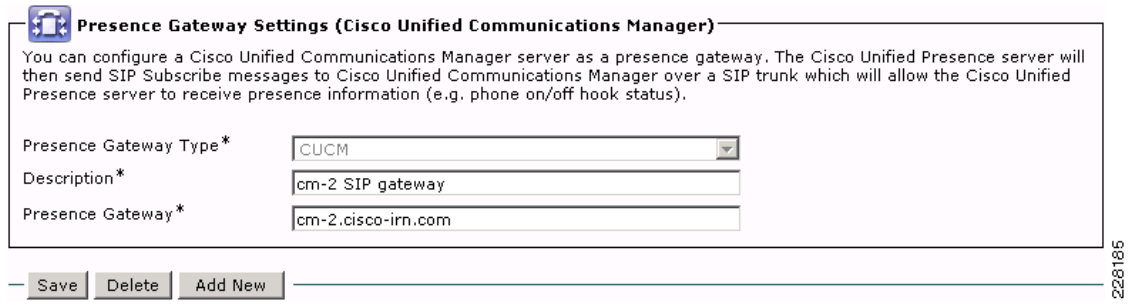
Step 3 And add routes to the Expert Advisor Runtime server. See Figure B-113.

Figure B-113



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

Figure B-114



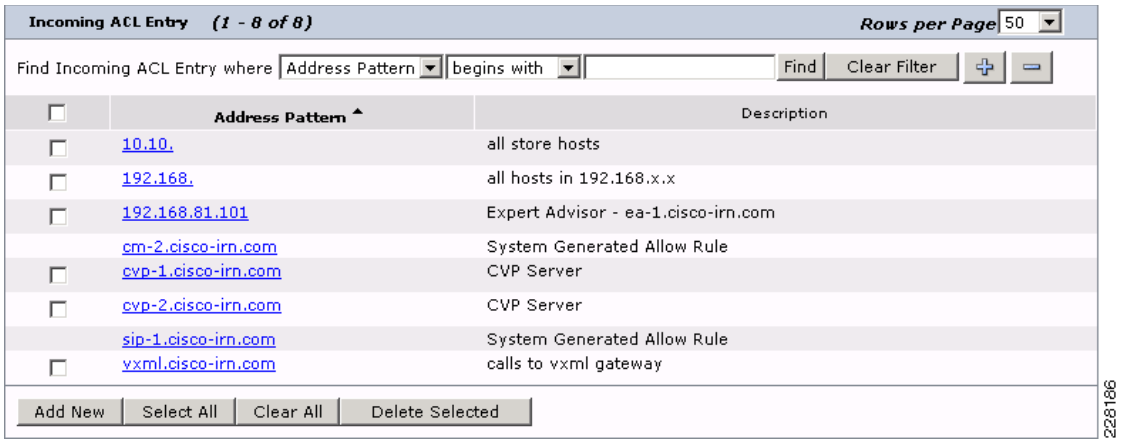
Step 5 Configure a Proxy Domain so that CUPC users can connect to the CUP server to obtain presence information. Go to **System > Service Parameters**.

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.

Step 8 Go to **System > Security > Incoming ACL**. See Figure B-115.

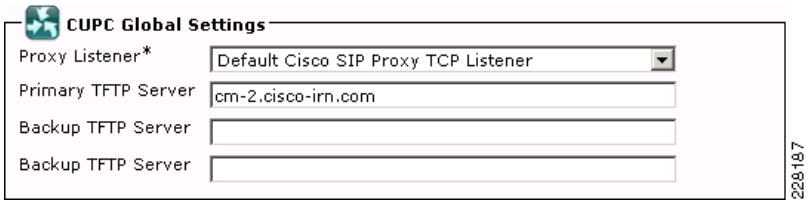
Figure B-115



Step 9 Configure TFTP Server for CUPC.

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

Figure B-116



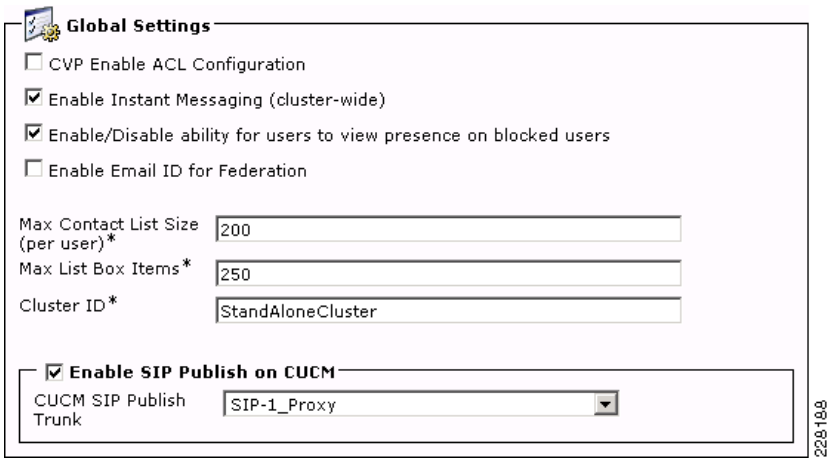
Step 11 Add SIP Publish capability to the SIP trunk between CUCM and CUP. This will allow CUCM to provide phone presence information to CUP server.

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.

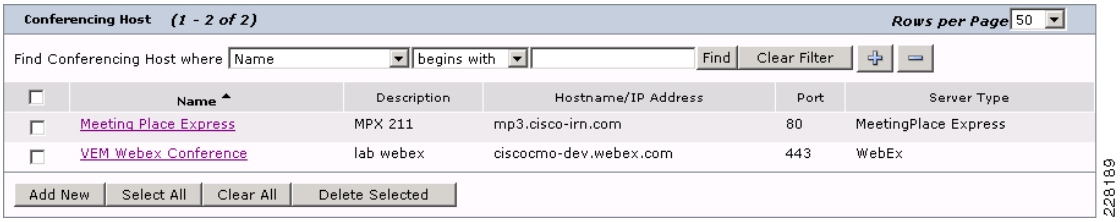
Figure B-117



Note 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**

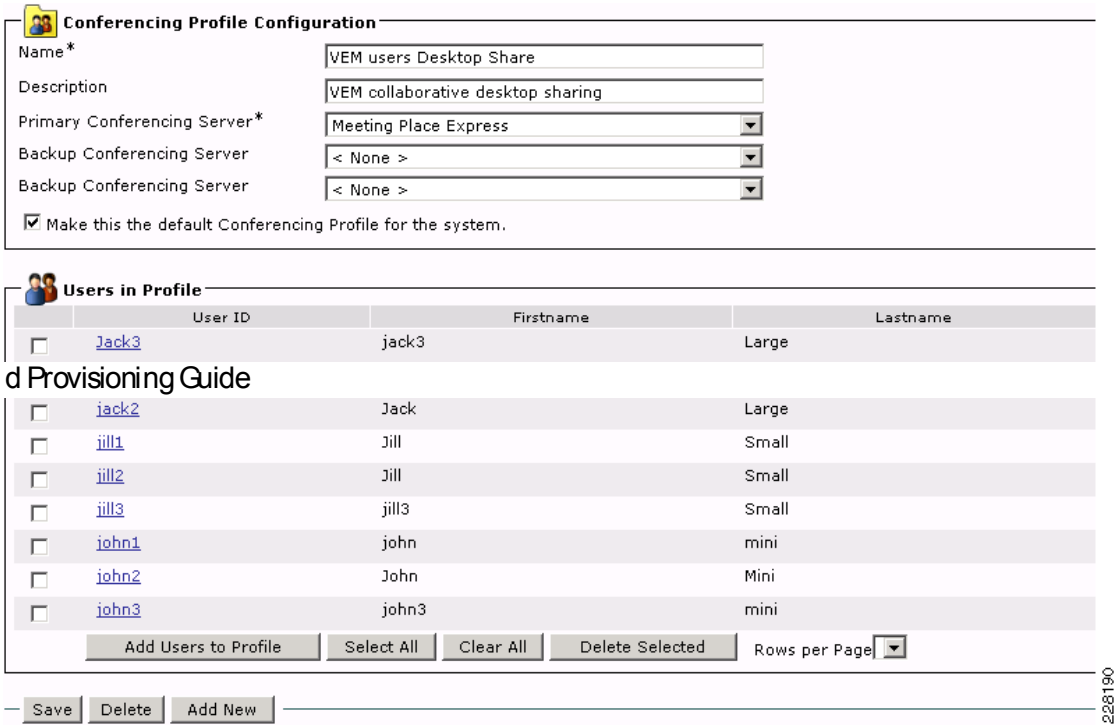
Step 15 Configure Conferencing hosts as appropriate. Go to **Application > Cisco Unified Personal Communicator > Conferencing Server**>New servers. See Figure B-118.

Figure B-118



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

Figure B-119



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

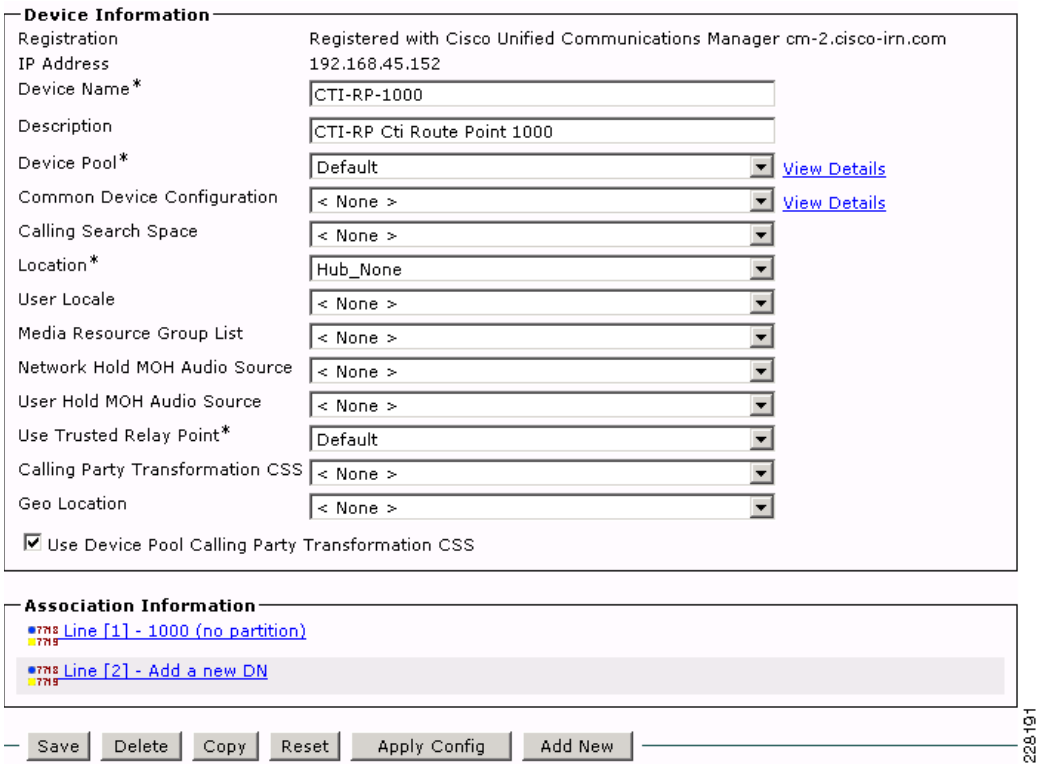
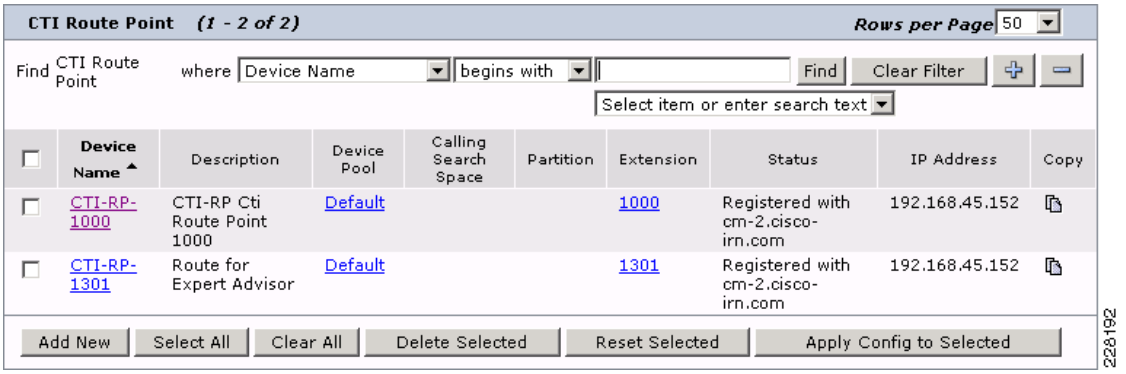
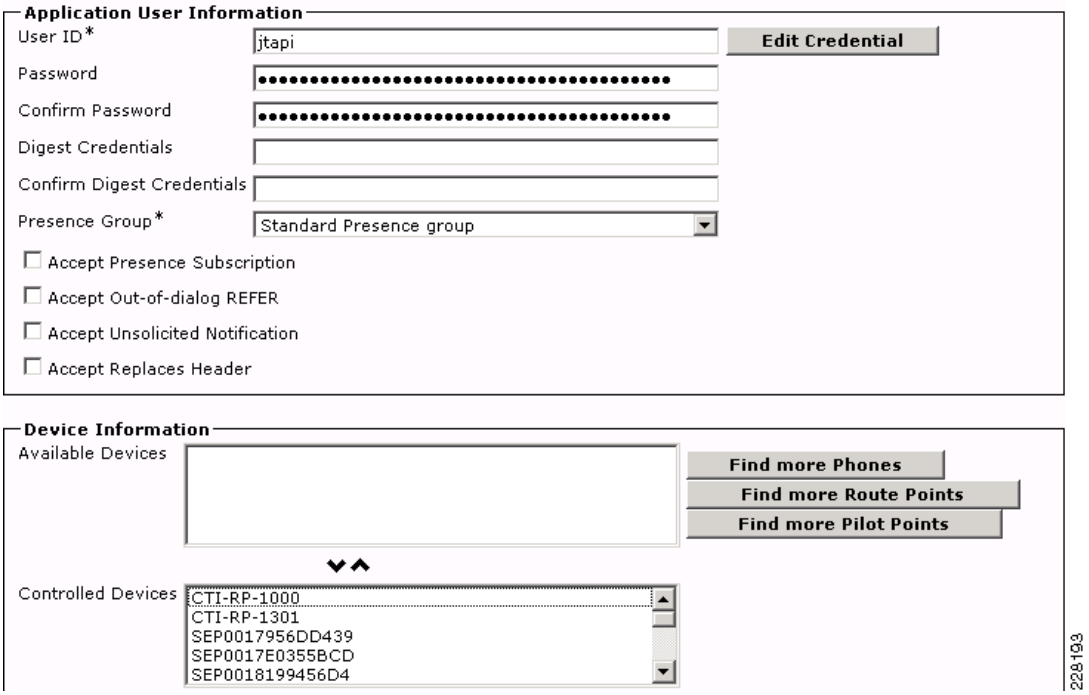


Figure B-121



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

Figure B-122



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

Figure B-123

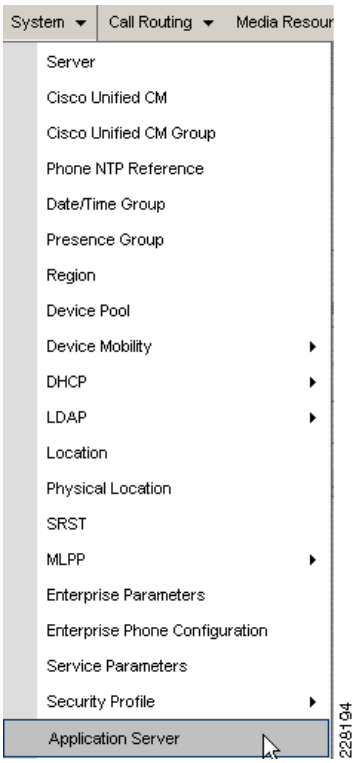
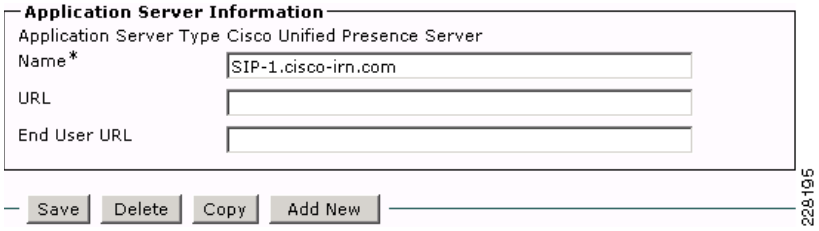
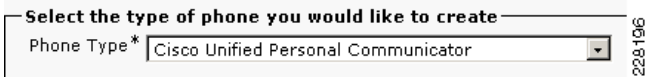


Figure B-124



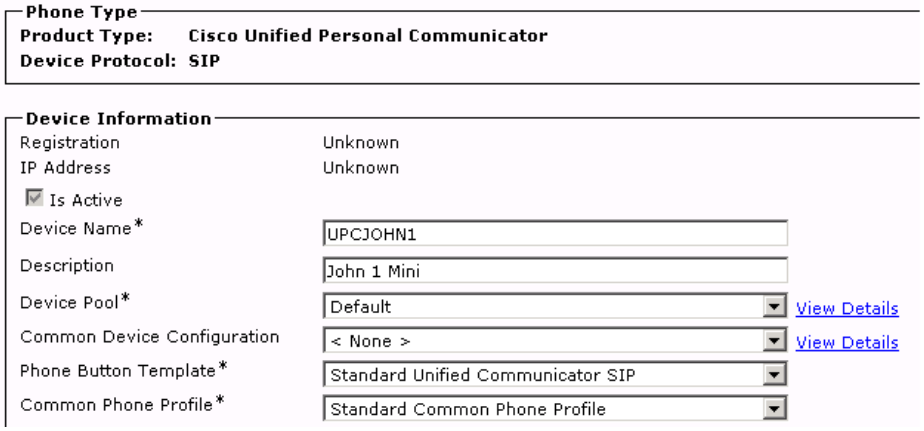
Step 3 If the expert advisor user will use CUPC as a softclient, create a phone device on CUCM for the CUPC softclients. Select the **Cisco Unified Personal Communicator** Phone Type. See Figure B-125.

Figure B-125



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.

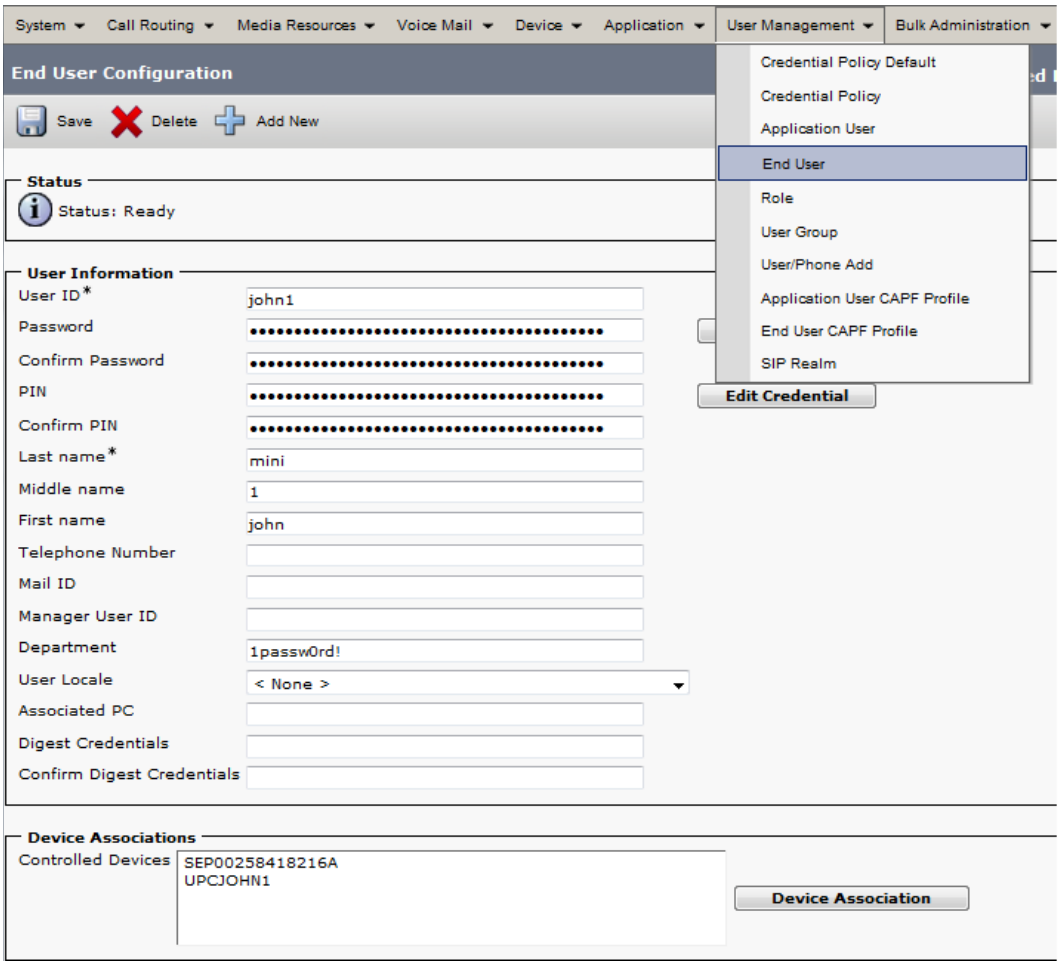
Figure B-126



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

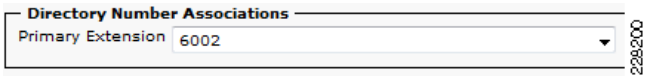
Step 6 Add expert advisor users as shown in Figure B-127.

Figure B-127



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

Figure B-128

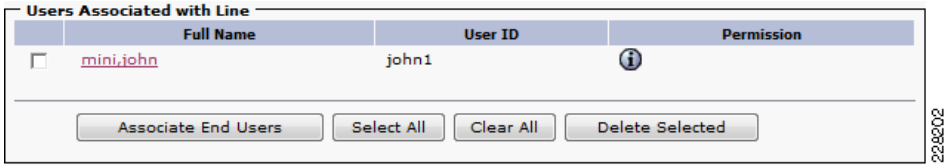


Step 8 If allowing CTI deskphone mode for the users, make the user part of the S**tandard CTI Enabled** user group. See Figure B-129.

Figure B-129

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.

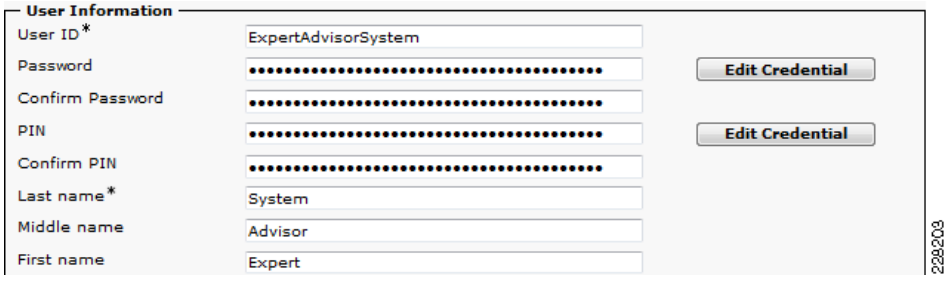
Figure B-130



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.

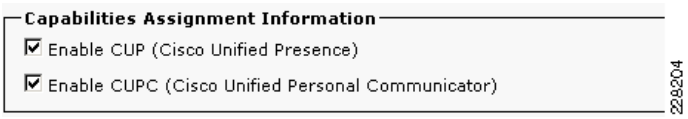
Figure B-131



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).

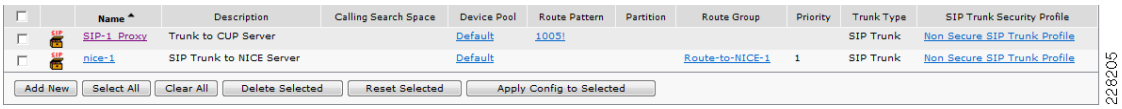
Step 12 In **System > Licensing > Capabilities Assignment**, enable CUP and CUPC for each Expert Advisor user. See Figure B-132.

Figure B-132



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



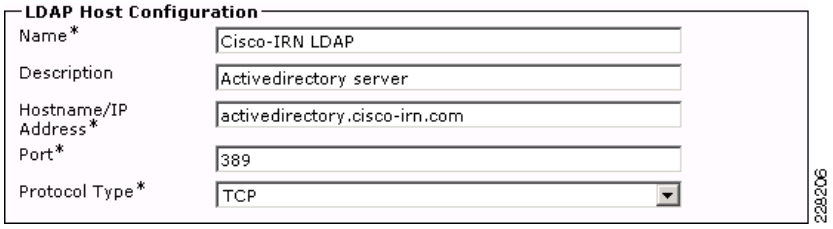
CUP Server Configuration

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.

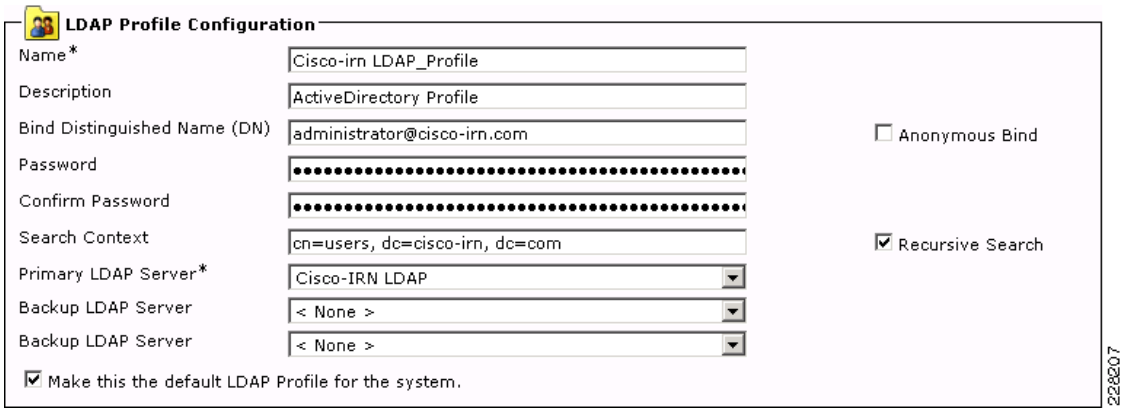
Figure B-134



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.

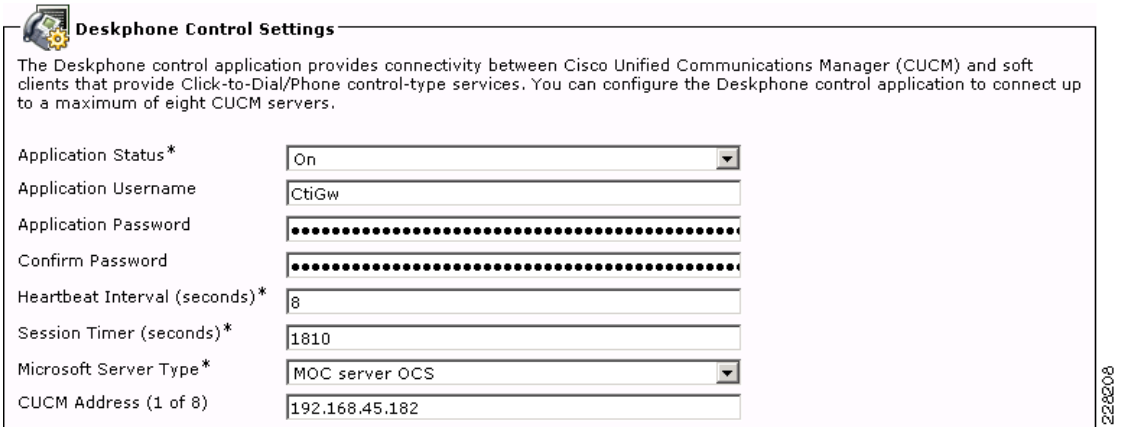
Figure B-135



Step 4 If you are deploying OCS/LCS and want to enable deskphone control with CUPC, go to **Application > Deskphone Control > Settings.**

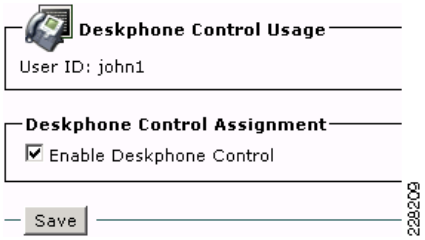
Step 5 Select **On** for the **Application Status** and enter the jtapi CtiGw information and CTIM information. See Figure B-136.

Figure B-136



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

Figure B-137

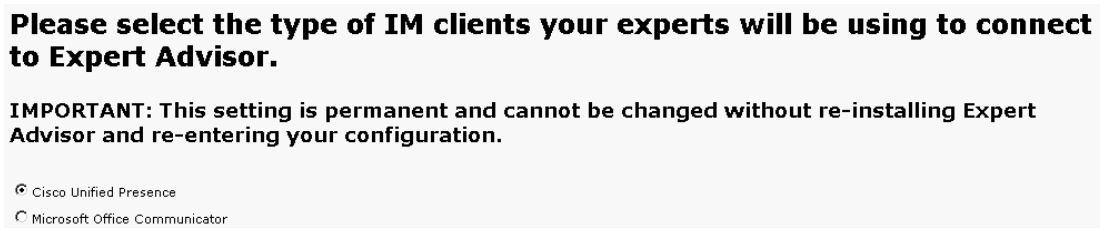


Note You do not have to go to **Application > Deskphone Control > Settings** in order to enable **Deskphone Control**, if you are not using OCS/LCS.

Expert Advisor Configuration

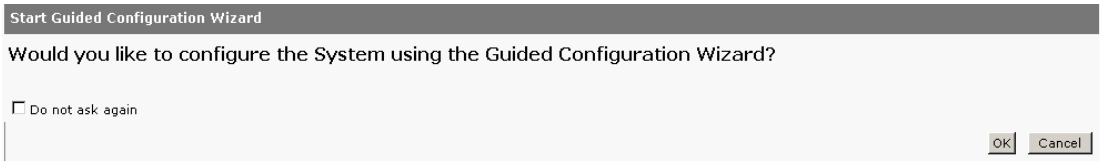
Step 1 Go to **http://**<*EA-ip-address*>. Expert Advisor system can be deployed with expert advisor users using either Cisco Unified Presence or Microsoft Office Communicator, not both types in the same Expert Advisor deployment. See Figure B-138.

Figure B-138



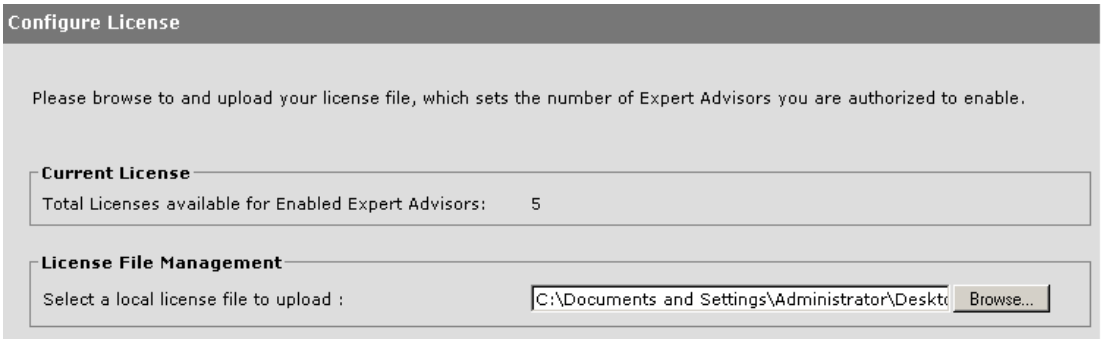
Step 2 Go through the Guided Configuration Wizard. See Figure B-139.

Figure B-139



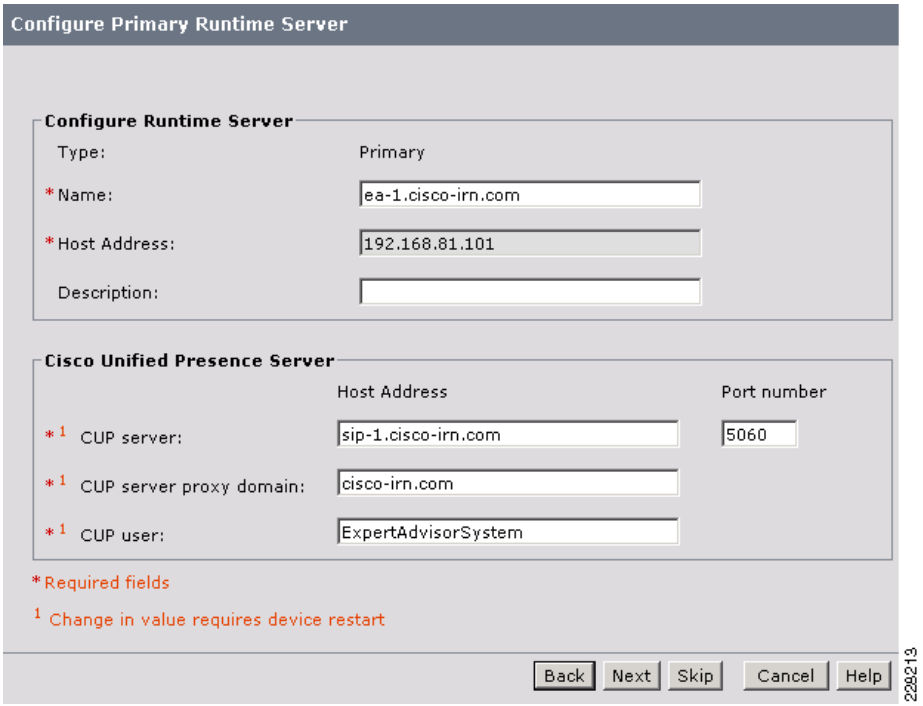
Step 3 Upload the license. If not, the system comes with a default license of 5 users. See Figure B-140.

Figure B-140



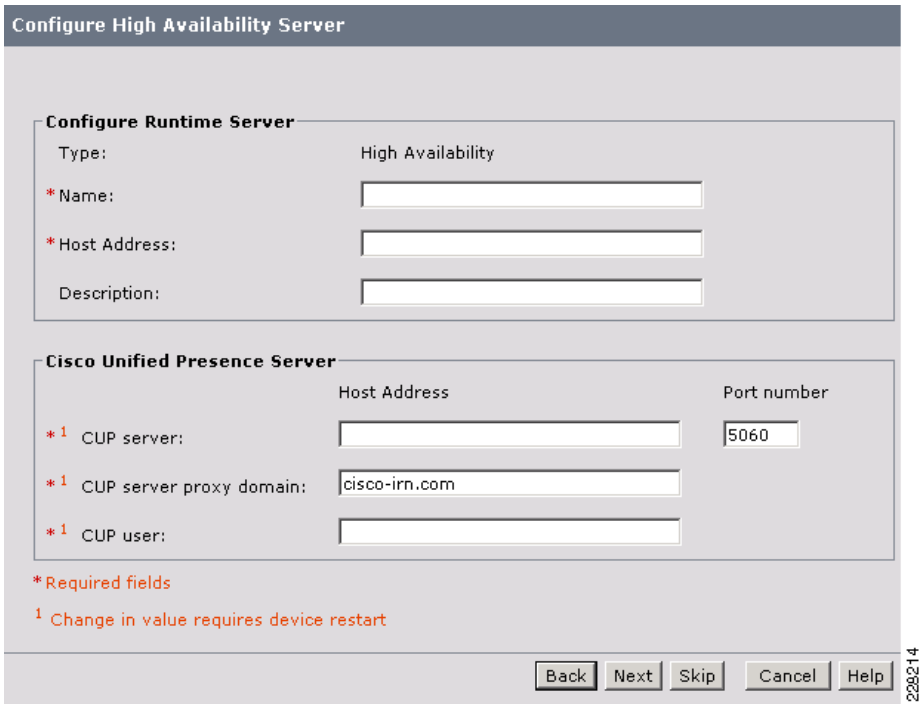
Step 4 Configure the Primary Runtime Server. In the *CUP user* field, enter the CUP user that Expert Advisor runtime server will use to connect to the CUP server. See Figure B-141.

Figure B-141



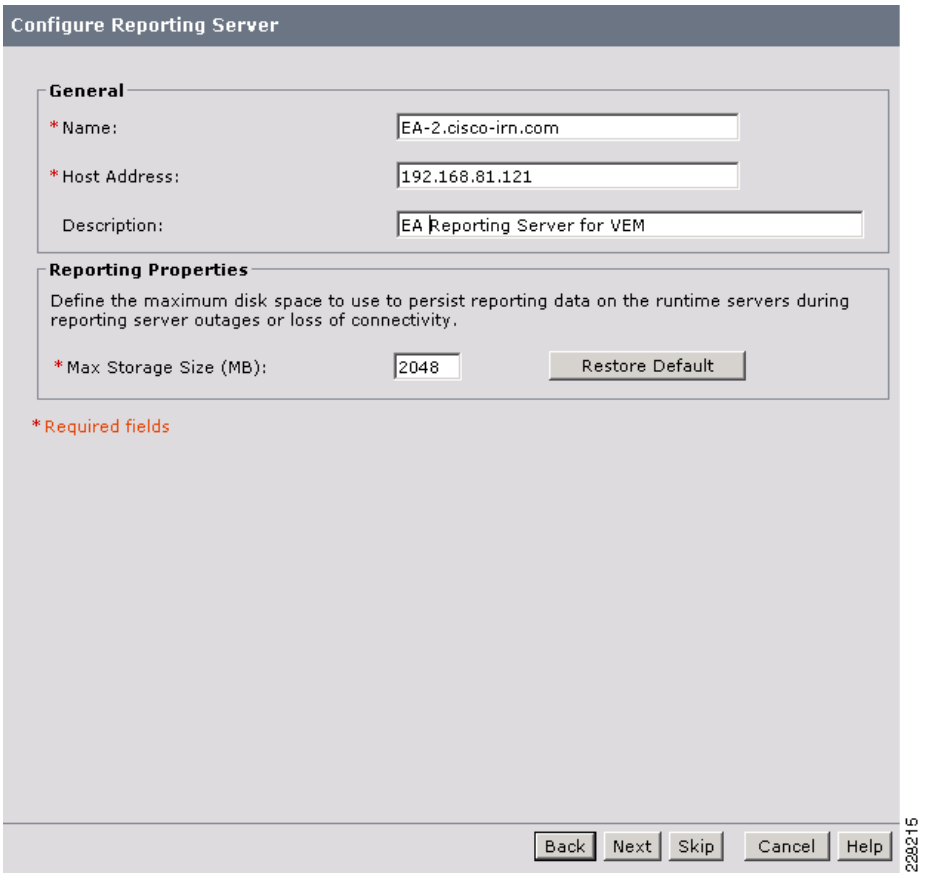
Step 5 Configure the secondary Runtime Server. Skip if you do not deploy a HA Runtime server.See Figure B-142.

Figure B-142



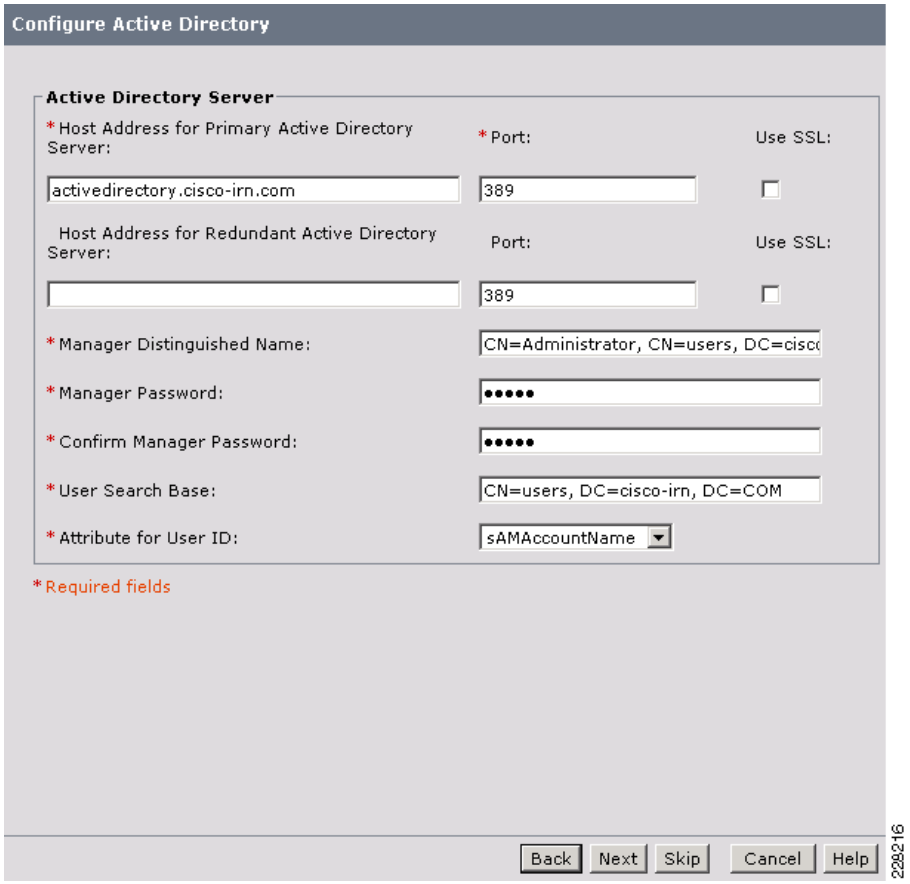
Step 6 Configure an Expert Advisor reporting server. Skip if you do not deploy a Expert Advisor reporting server. See Figure B-143.

Figure B-143



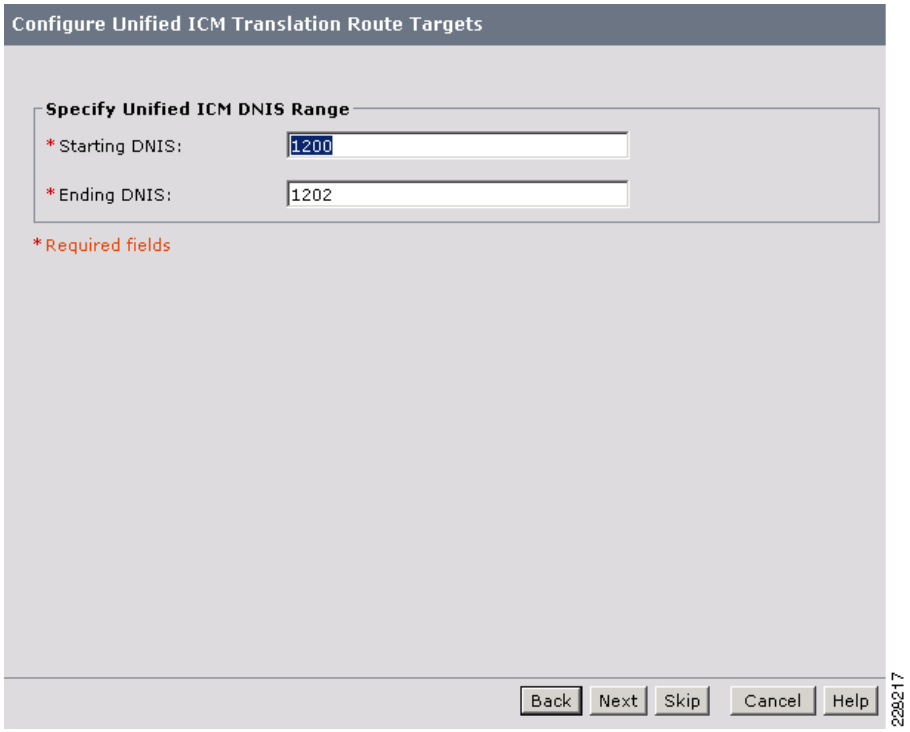
Step 7 Configure a AD server. See Figure B-144.

Figure B-144



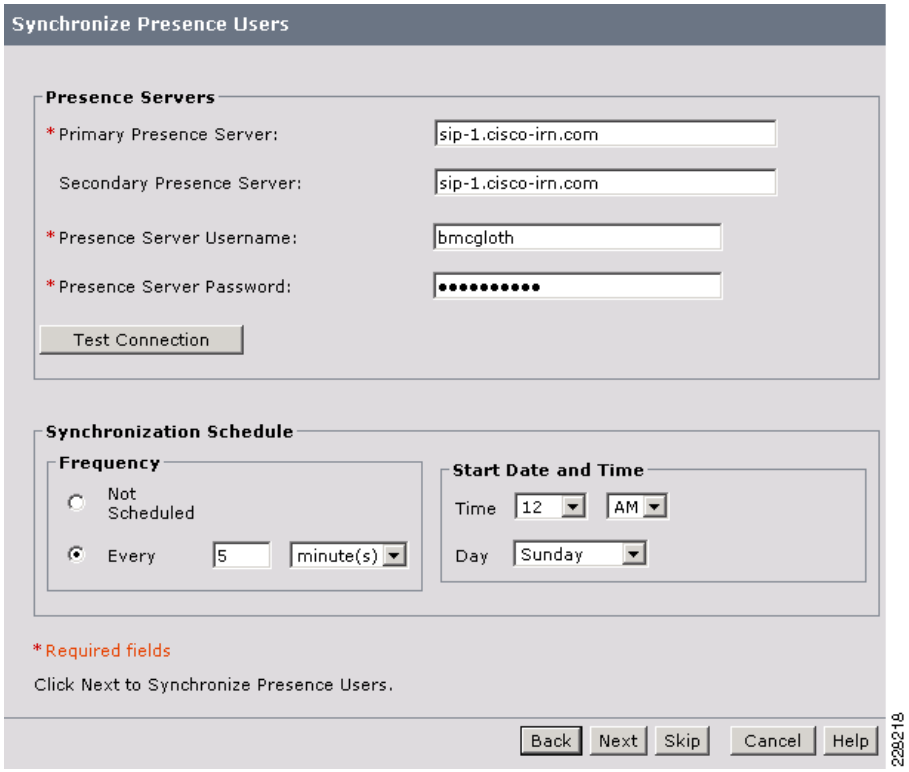
Step 8 Configure the ICM translation route. These DNIS numbers need to be routable by your system (for example, enter a route in CUP SIP proxy). See Figure B-145.

Figure B-145



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

Figure B-146



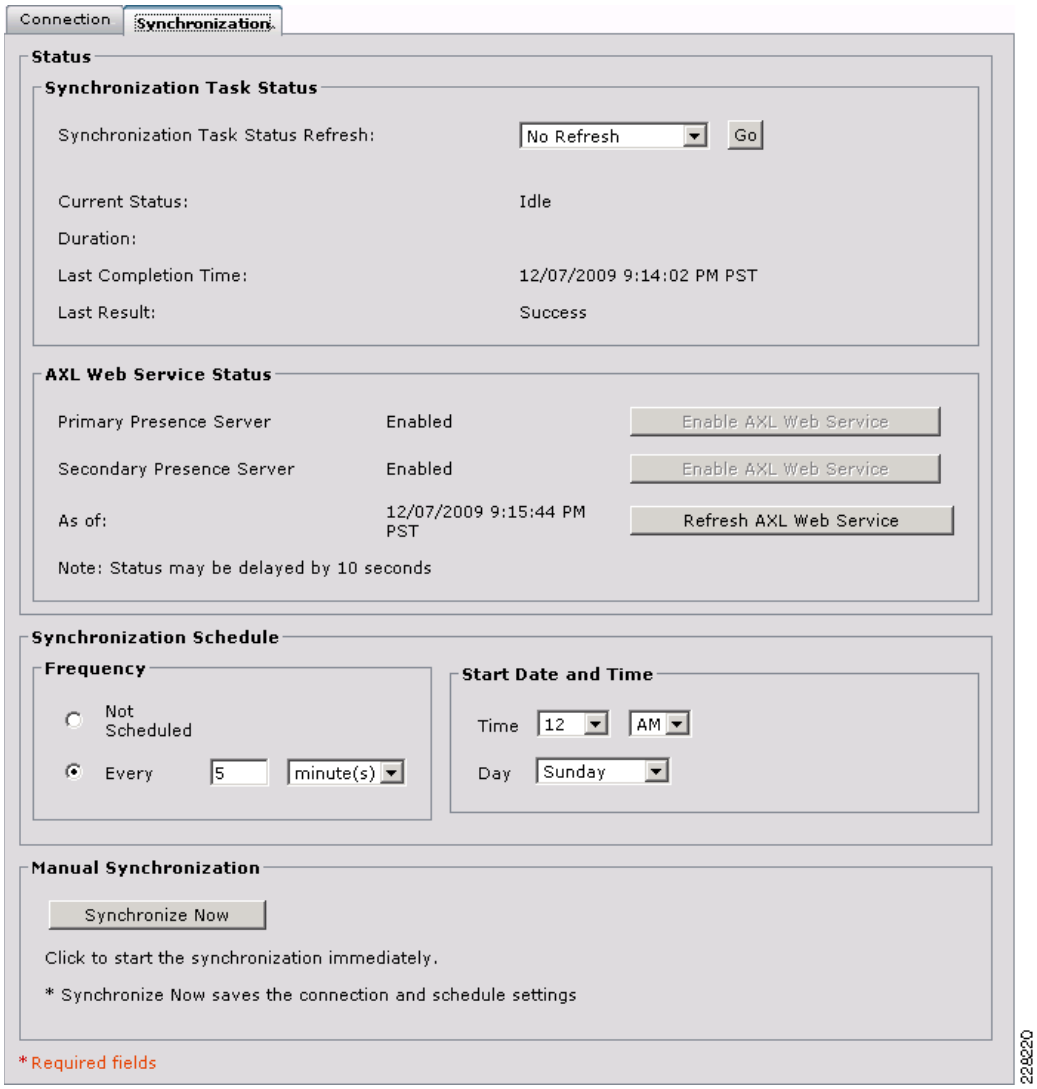
Step 10 Verify the summary. See Figure B-147.

Figure B-147

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.

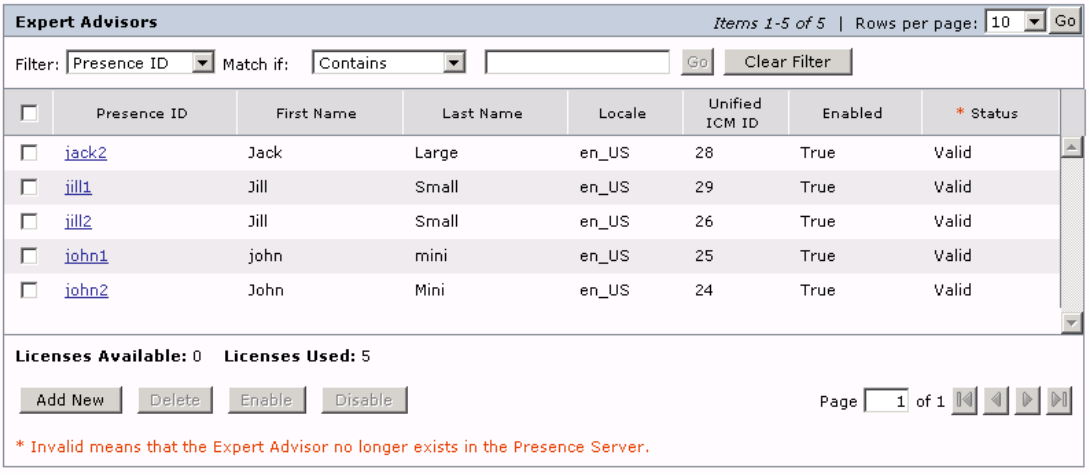
Figure B-148



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

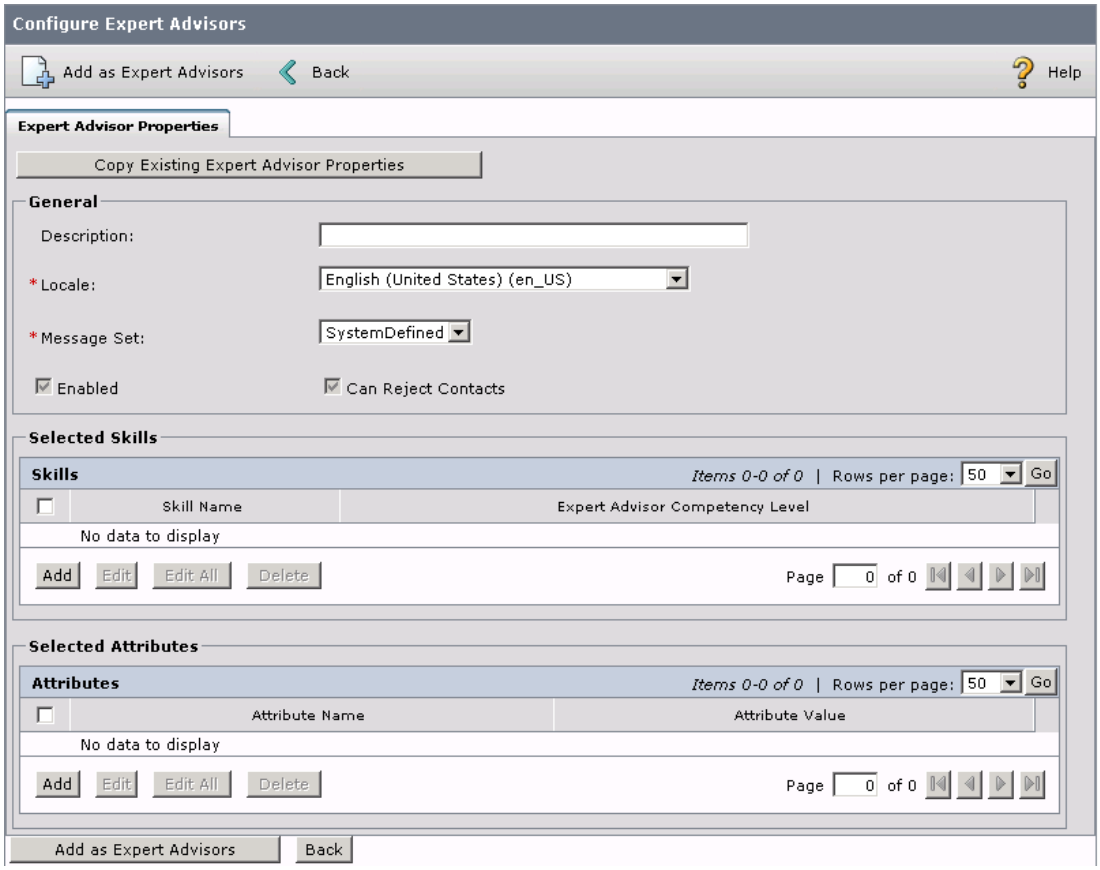
Step 14 Click on **Add New**. Select the users from CUP. See Figure B-149.

Figure B-149



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

Figure B-150



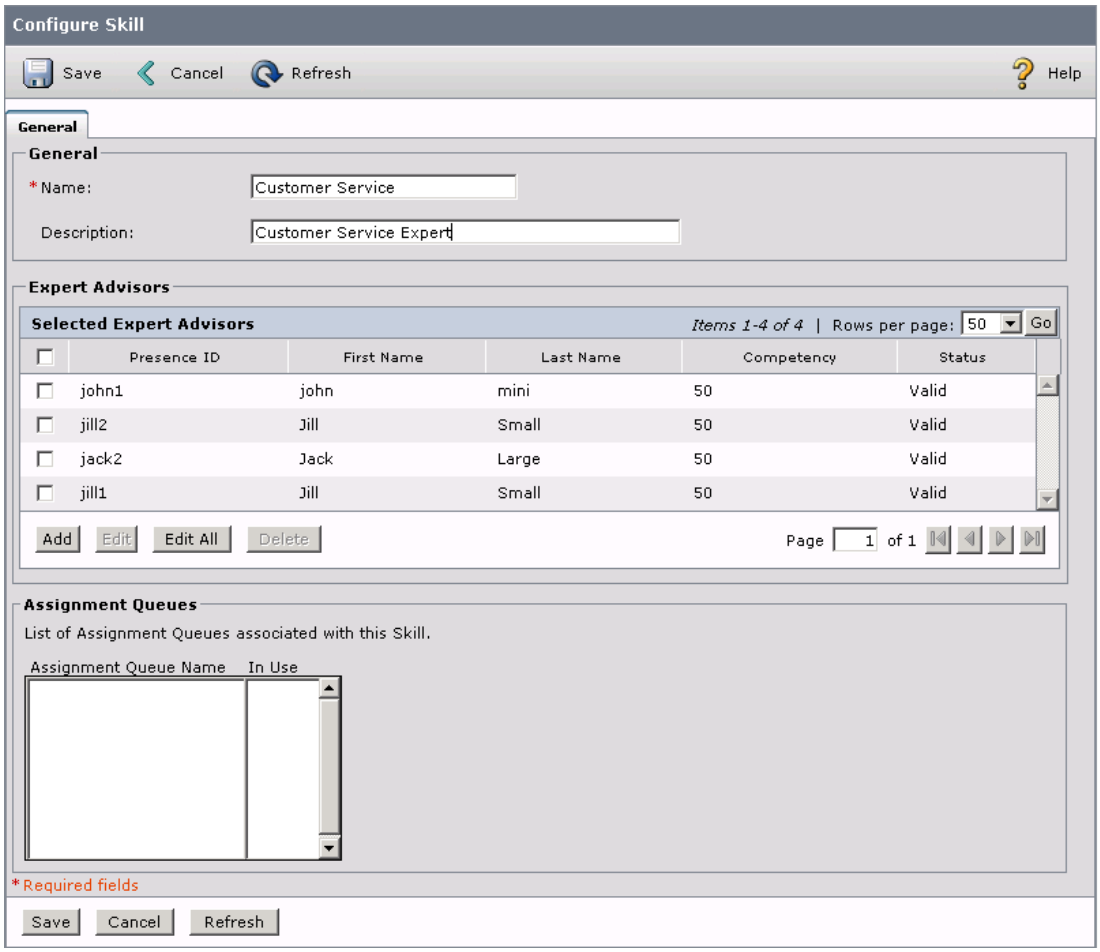
Step 16 In **Daily Management**, select **Skills**. Click on **Add New**.

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.

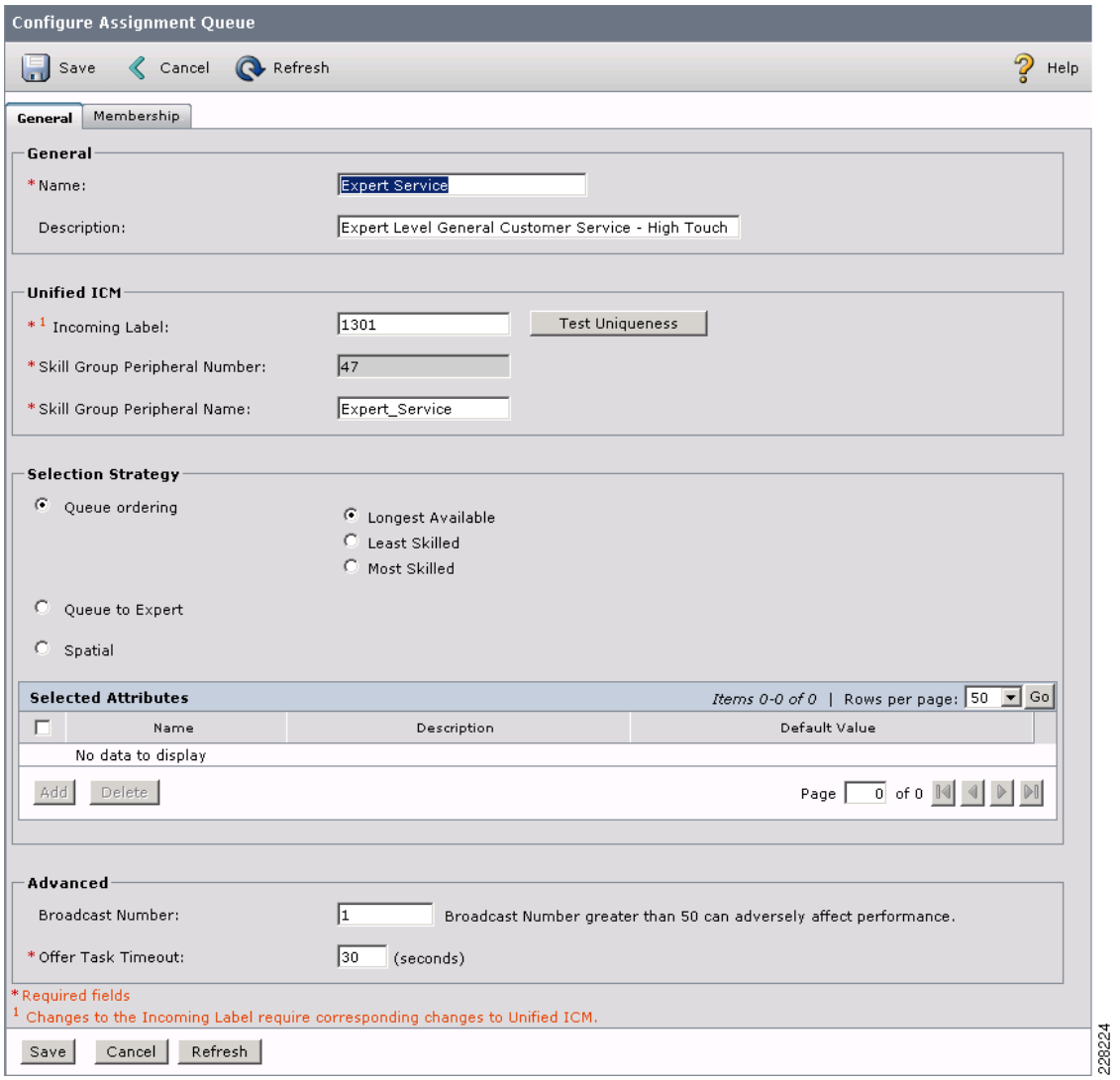
Figure B-151



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.

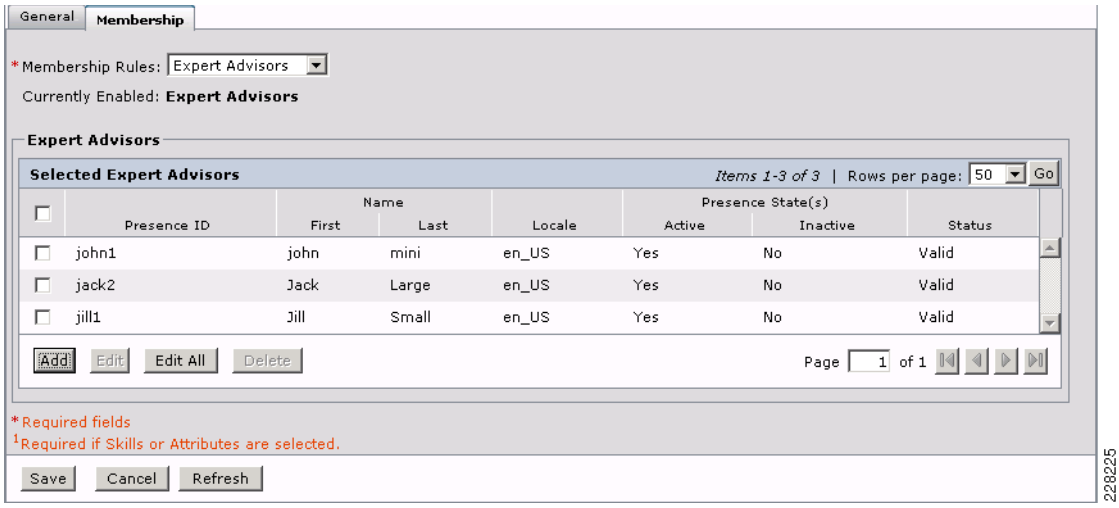
Figure B-152



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.

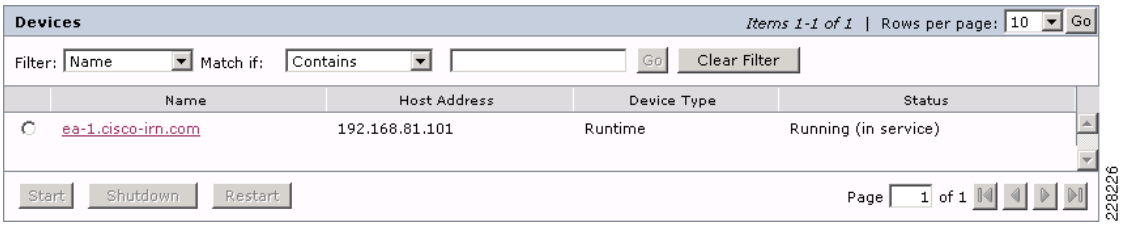
Figure B-153



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



ICM Configuration

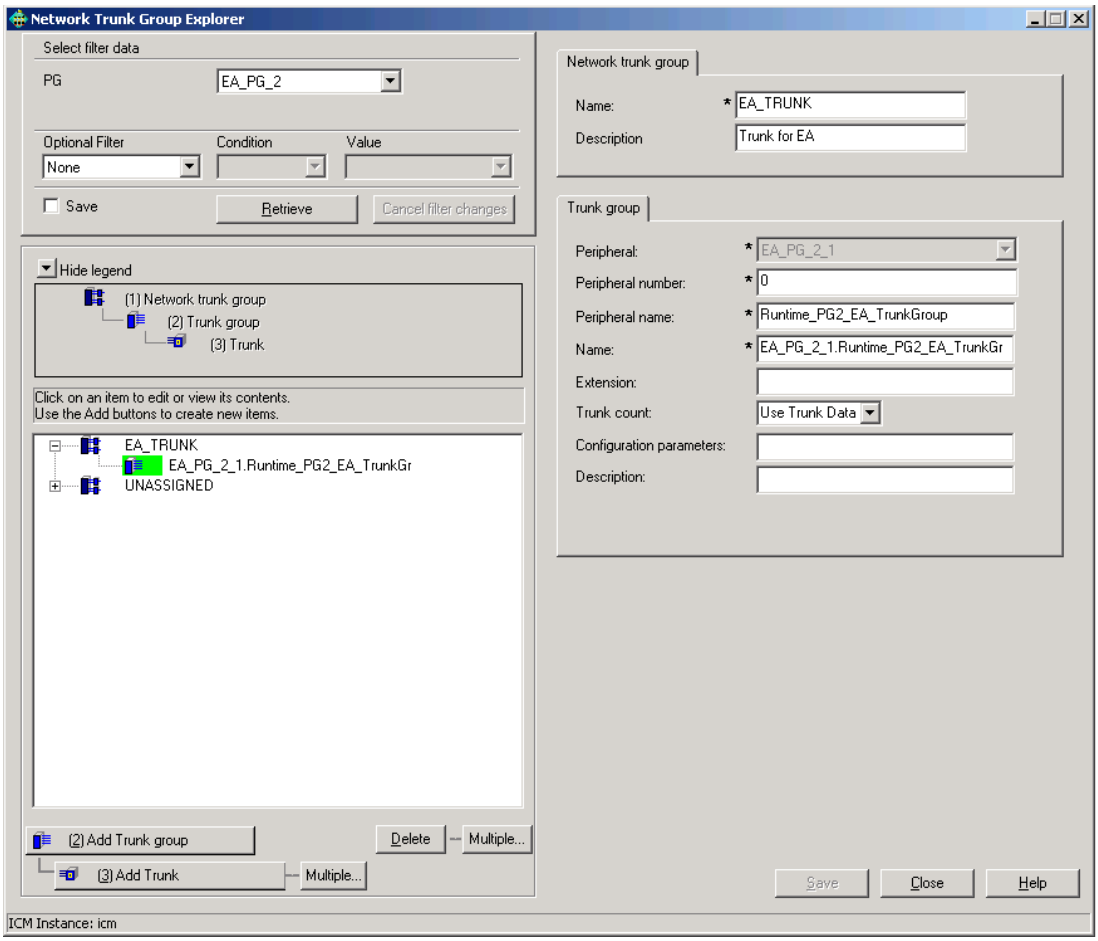
To configure ICM, complete the following steps:

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.

Figure B-155



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.

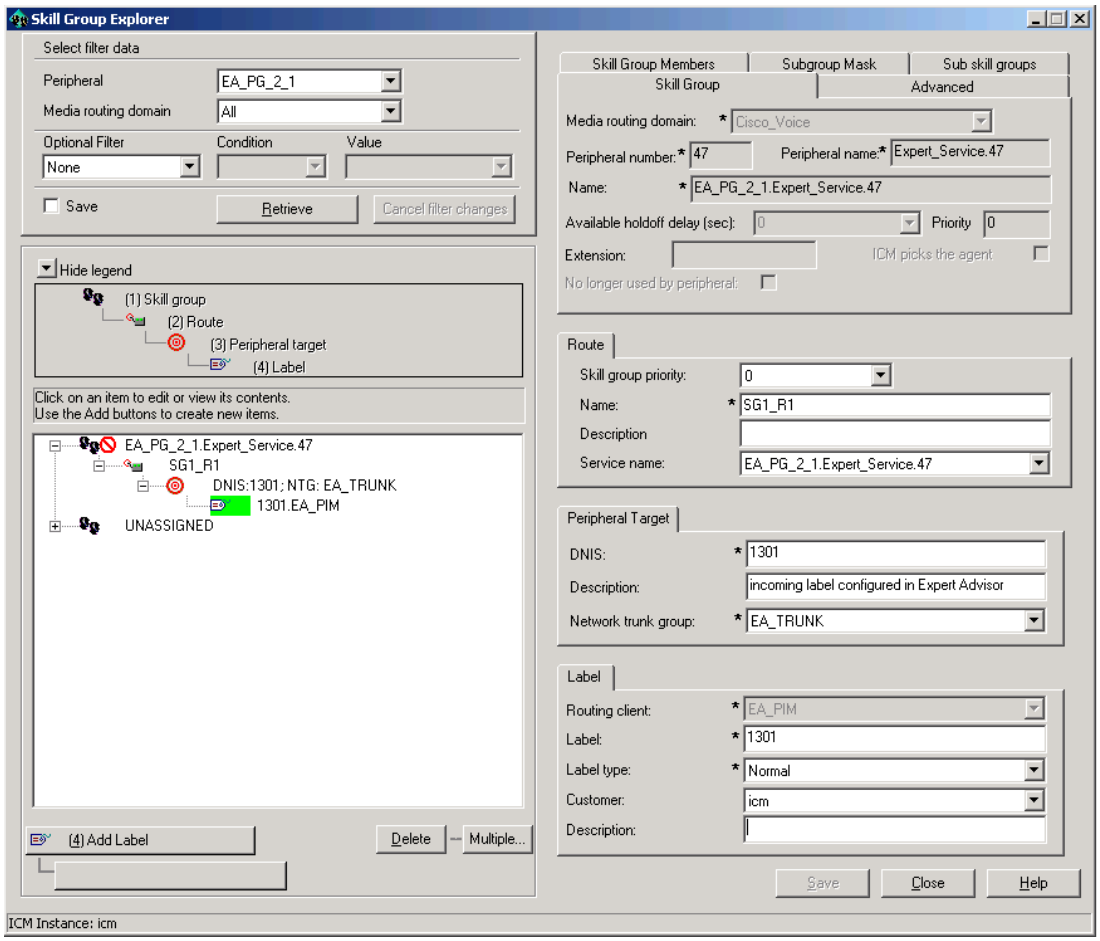
Step 9 Enter the DNIS that should be the same as the Incoming Label configured on Expert Advisor Operations Console.

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.

Figure B-156



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**.

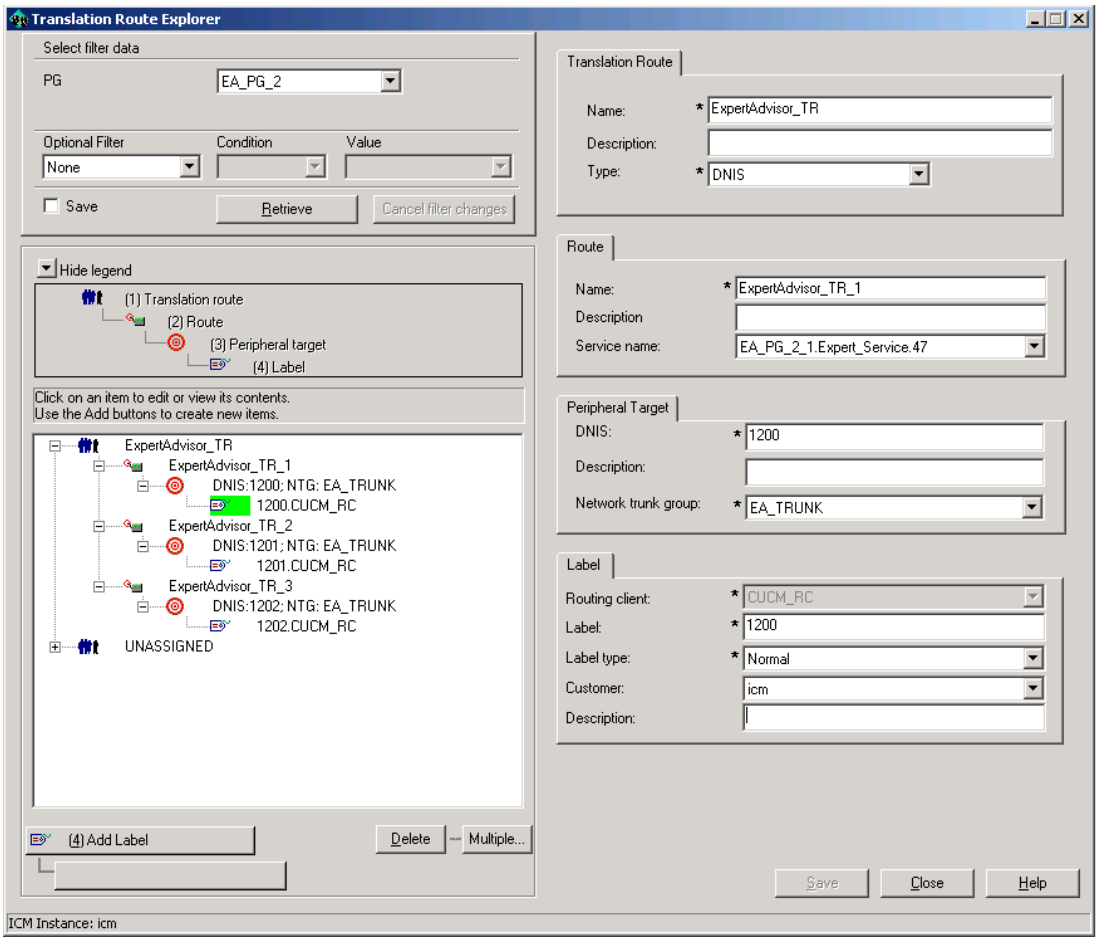
Step 16 Enter a name for the Route and click on **Save**.

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.

Figure B-157



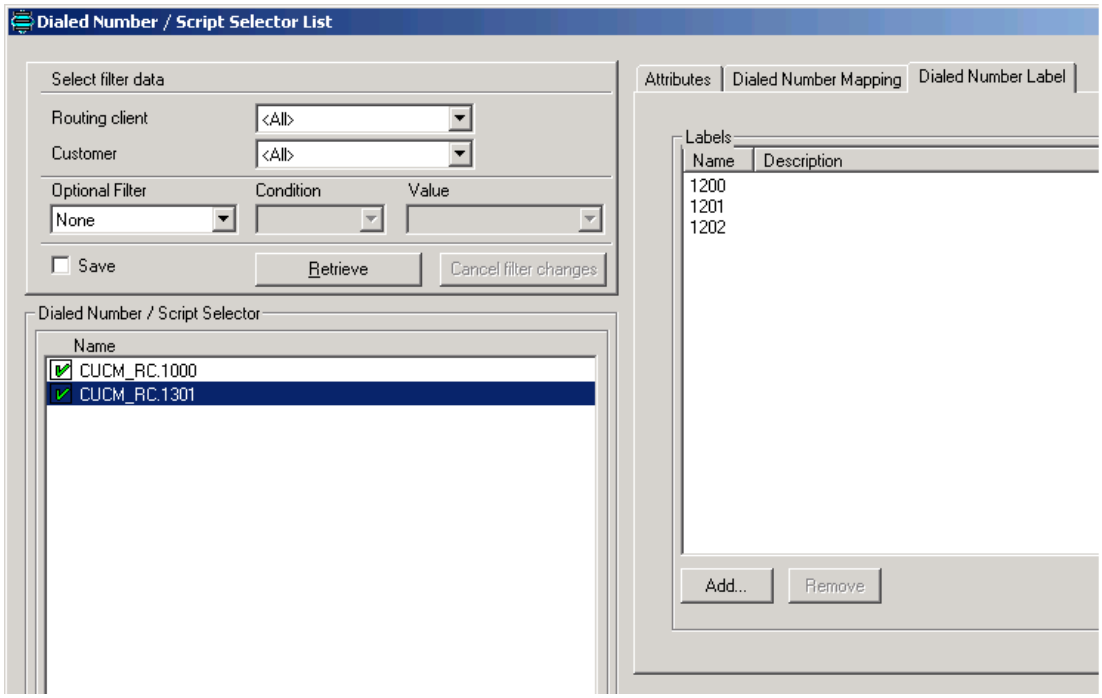
Step 20 Edit the Dialed Number for the Expert Advisor. This is the number that customer or agent will dial to reach an expert advisor user.

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.

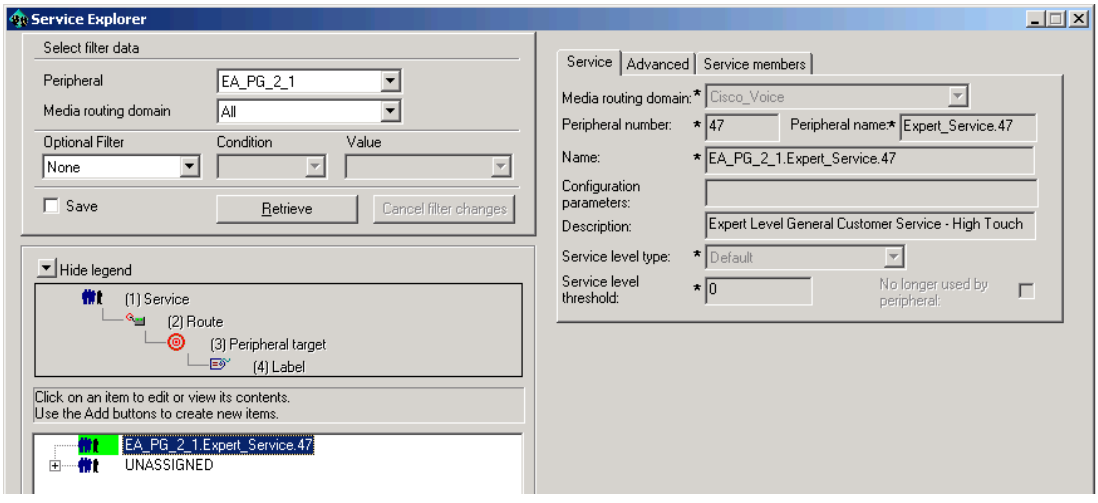
Figure B-158



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.

Figure B-159



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.

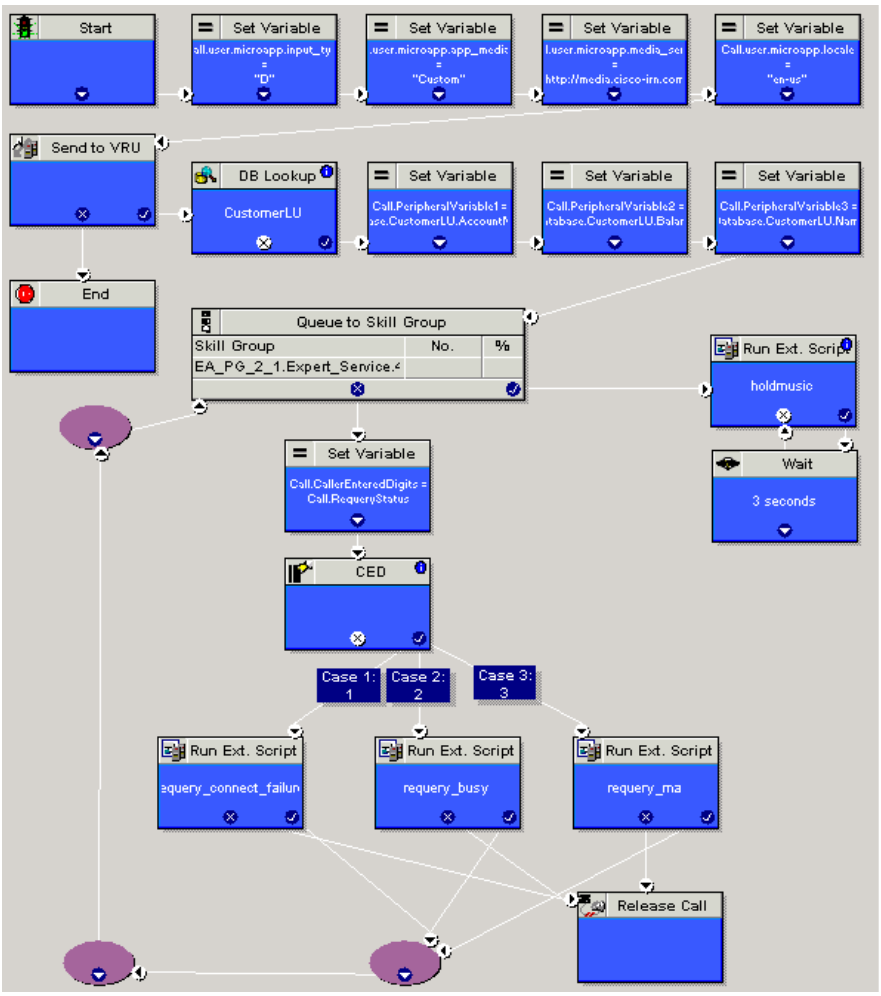
Step 7 Perform a DB lookup based on the calling number and/or caller entered digits for an account number.

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.

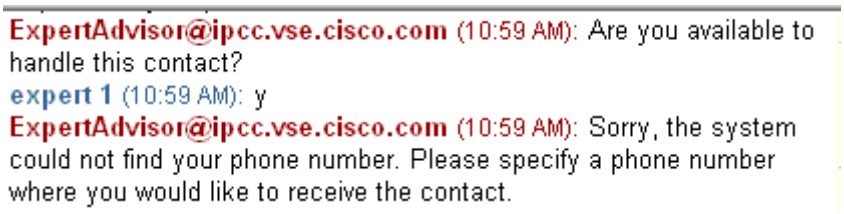
Figure B-160



Trouble Shooting Tip

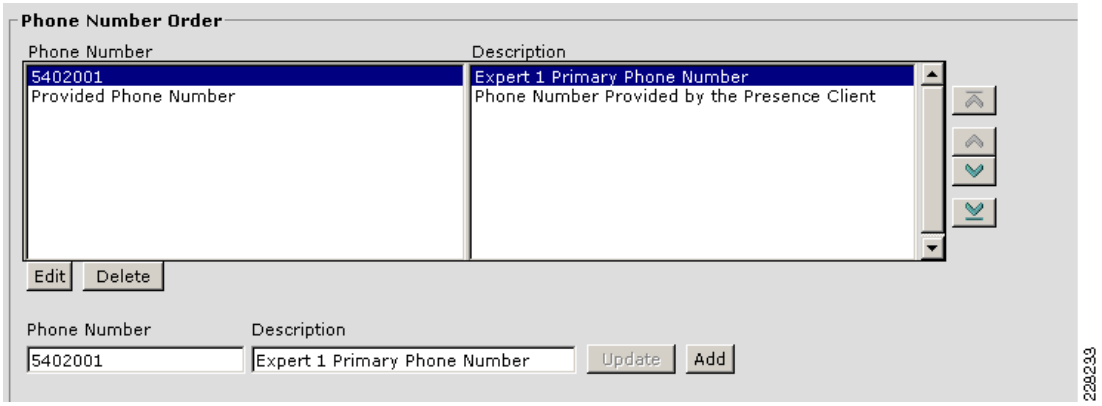
If using CUPC in the deskphone mode, you might see the following error message when the expert advisor is replying with a "**Yes**" that you will not see in the softphone mode. See Figure B-161.

Figure B-161



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

Figure B-162

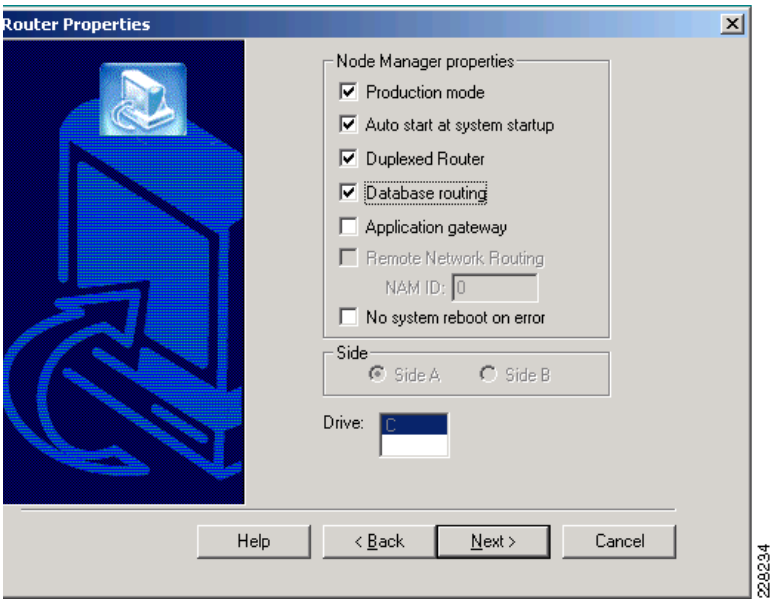


Database Lookup and Passing Data to the Expert

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



Step 3 On the ICM Router server, open the regedit utility and edit the registry key for the Database configuration as follows:

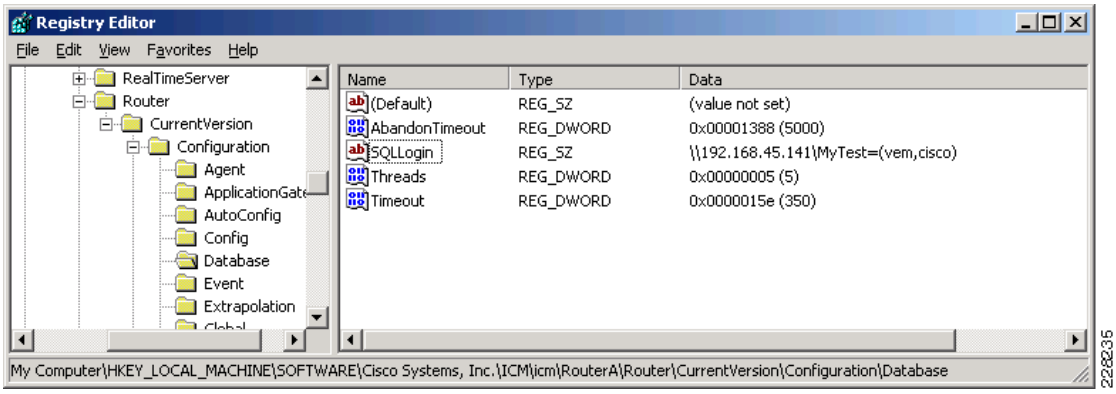
a. Locate **HKEY_LOCAL_MARCHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<instance>\RouterA\Router\CurrentVersion\Configuration\Database**.

b. For the SQLLogin key, enter the information of your database:

\\<*ipaddress-or-name*>\<*Database_name*>=(<*username*>, <*password*>)

Figure B-164.

Figure B-164

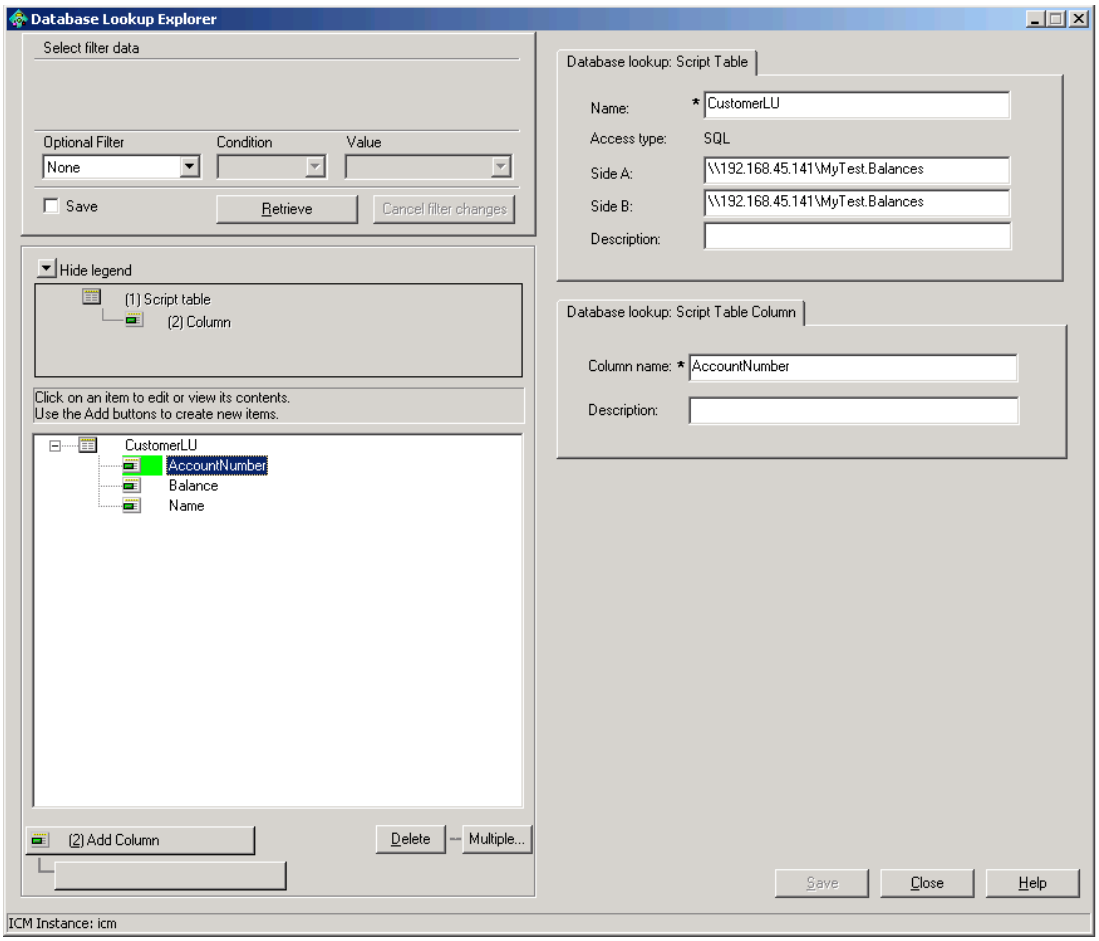


Note You need to do that only on one side. This setting will be automatically replicated to the other side.

Step 4 In ICM Configuration, open the DB Lookup Explorer.

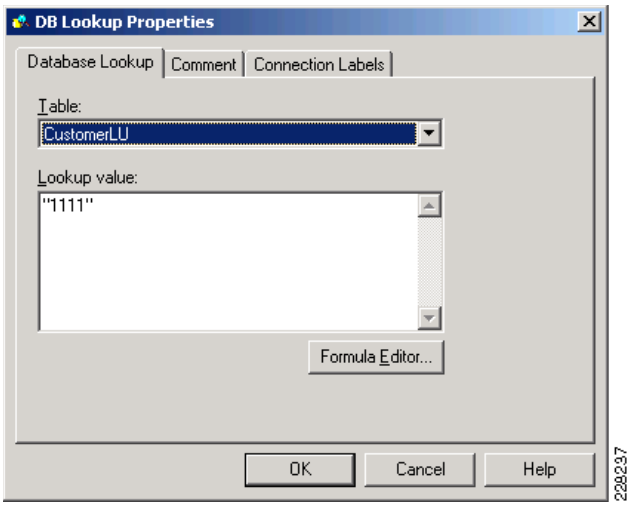
Step 5 Enter a name for the Script Table. For side A and B, enter the DB server information with DB name and table as: \\<*IPorHostname*>\<DB>.<*Table*>. See Figure B-165.

Figure B-165



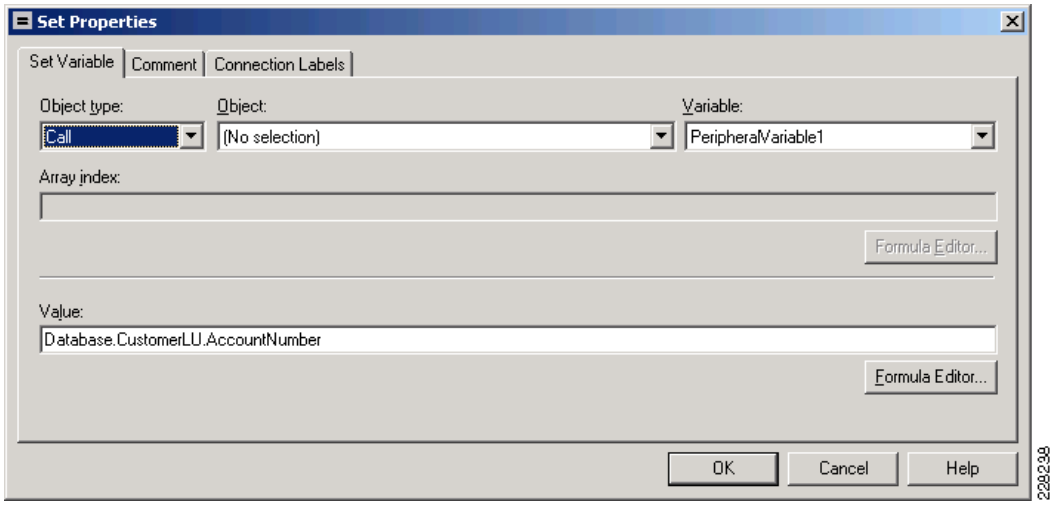
Step 6 In the ICM script, perform add a DB Lookup step to select the row you are looking for. For example, if the account number should match "1111", then enter the following information in the Database Lookup step. See Figure B-166.

Figure B-166



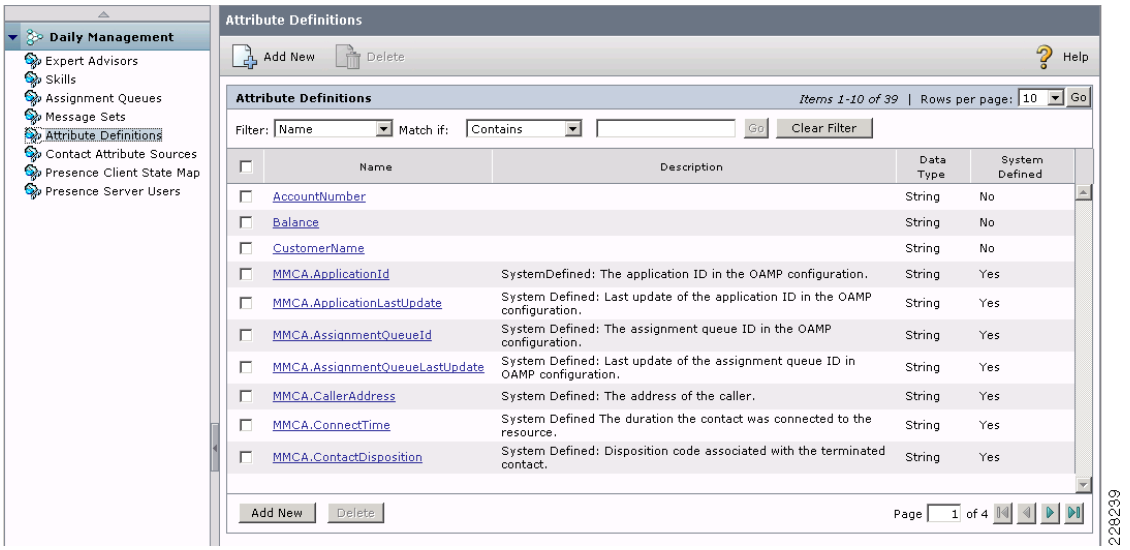
Step 7 After a match is found other column data can be retrieved for this record. In the following example, we set the *PeripheralVariable1* to the AccountNumber column of the DB record, using the **set** step. Later on, with Expert Advisor, we will map this Peripheral Variable1 to an Expert Advisor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

Figure B-167



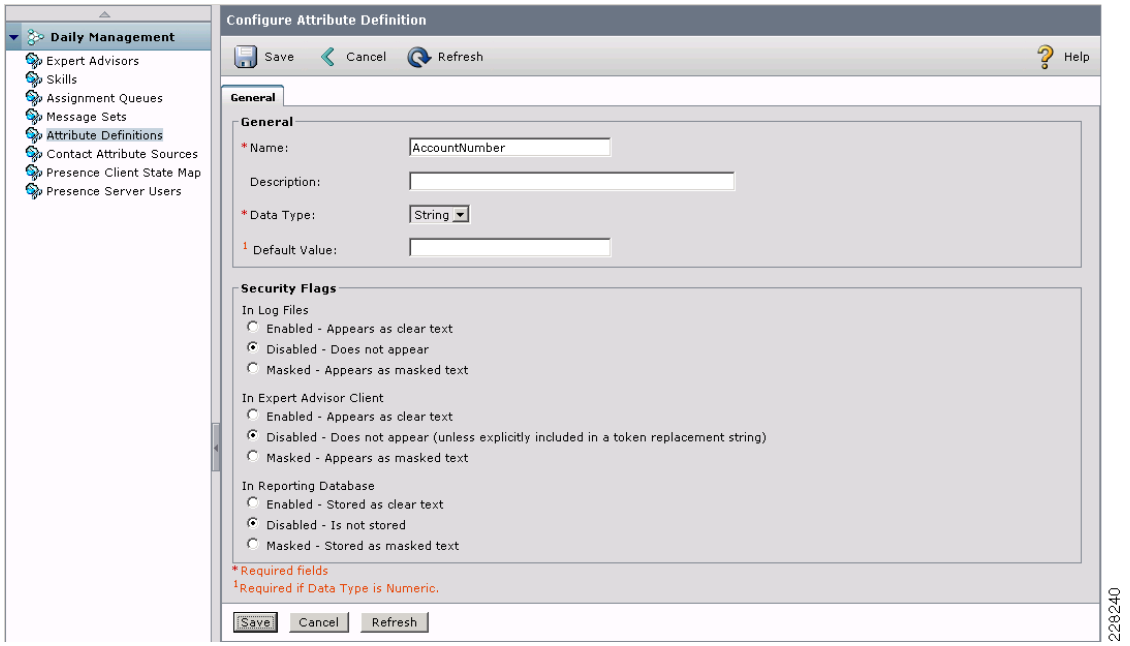
Step 8 On Expert Advisor OAMP, if you want to display this information to the expert, create new Attribute Definitions. Go to **Daily Management**, select **Attribute Definitions**. See Figure B-168.

Figure B-168



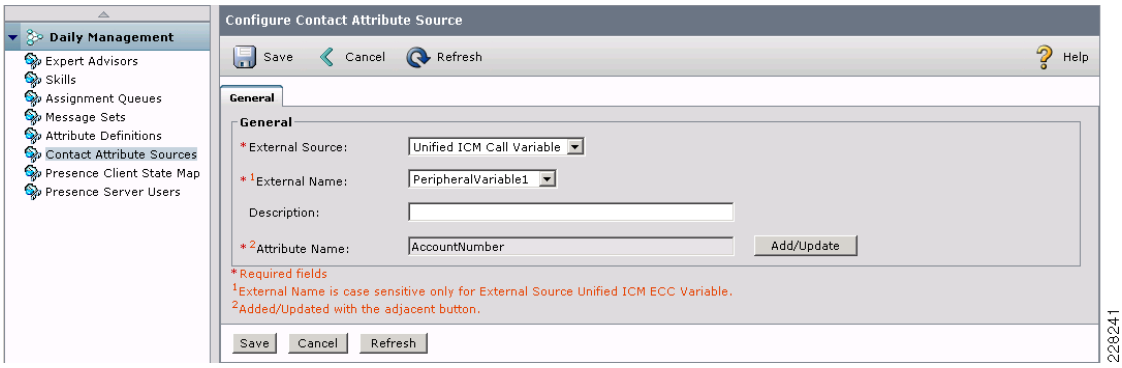
Step 9 Add new attribute definitions. Click on **Disabled** in the **In Expert Advisor Client**. See Figure B-169.

Figure B-169



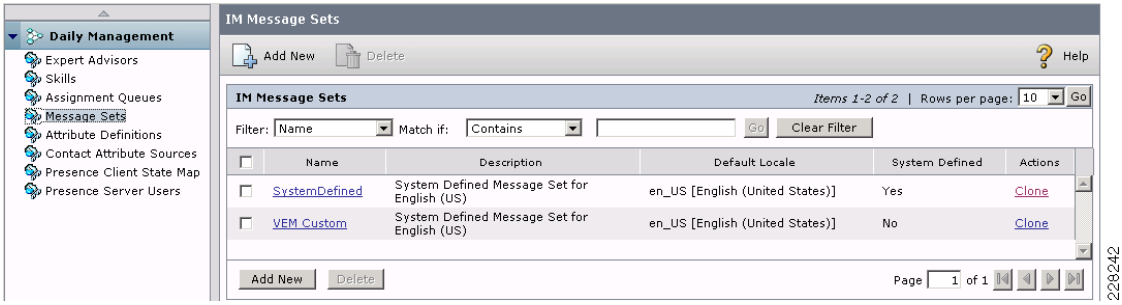
Step 10 In Contact Attribute Sources, map the new Attribute Definitions to Variables you use in the ICM script. See Figure B-170.

Figure B-170



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

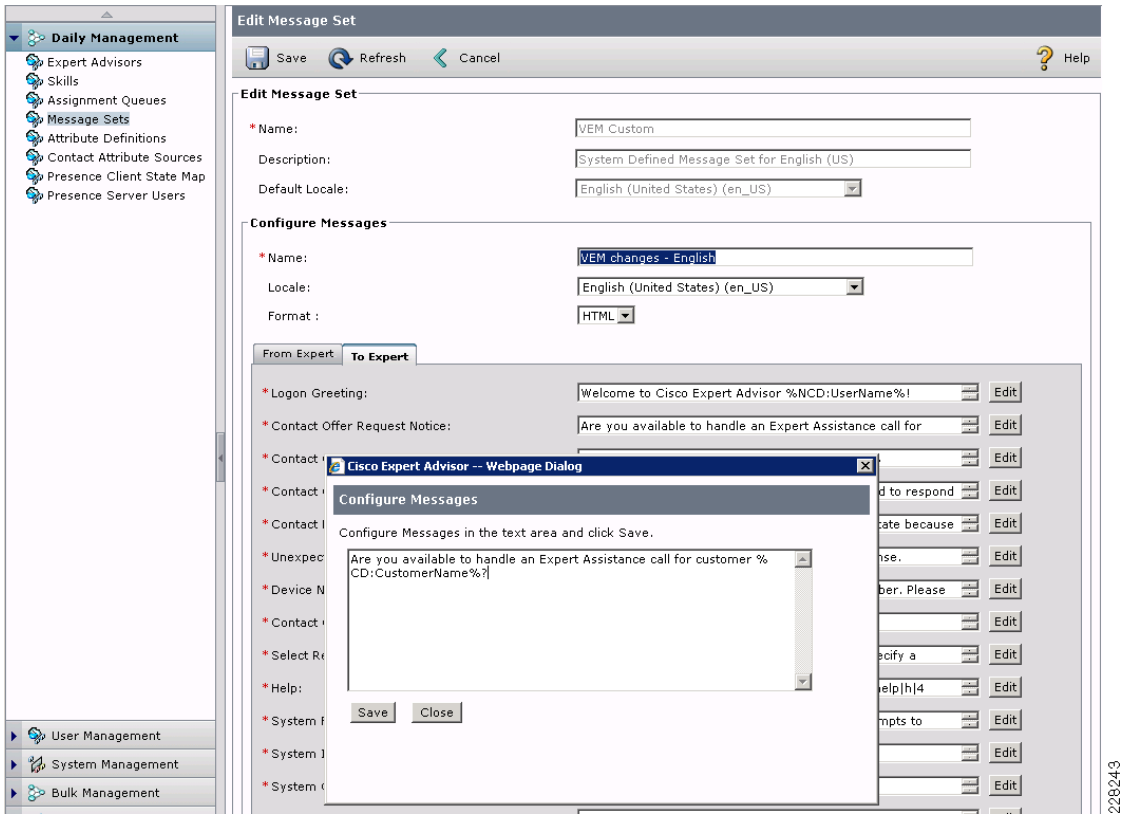


Step 12 Edit the new message set and choose the **To Expert** tab.

Step 13 Edit the **Contact Offer Request Notice**.

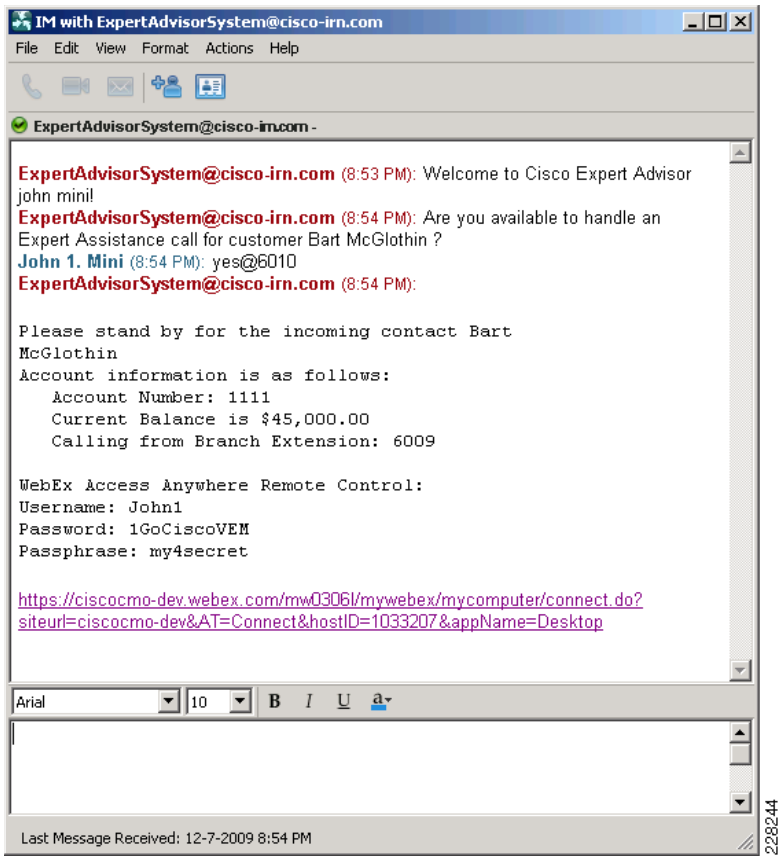
Step 14 Edit the **Contact Offer Notice**. See Figure B-172.

Figure B-172



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

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

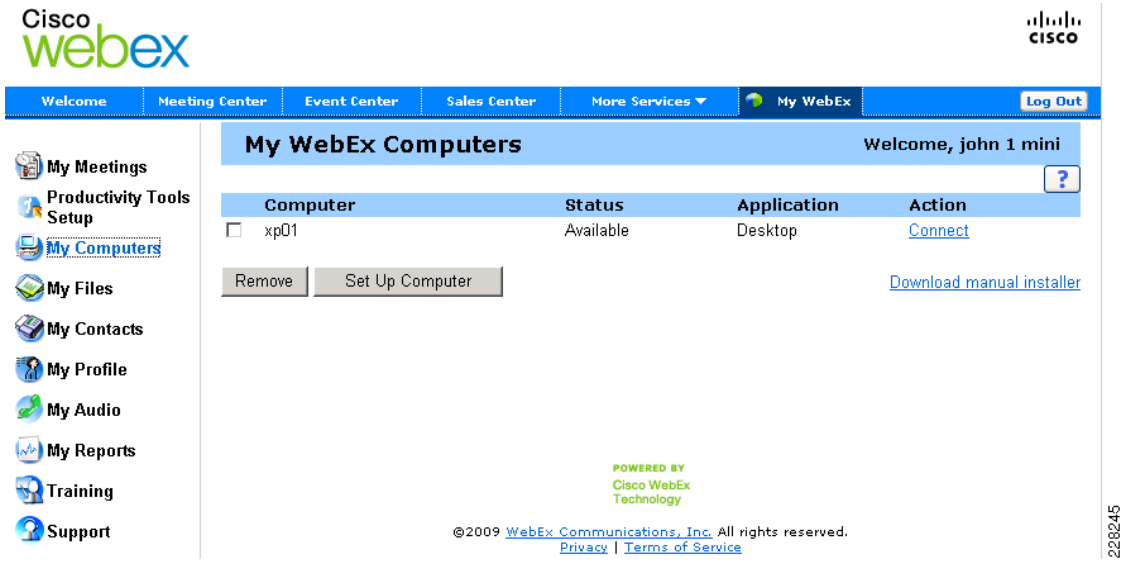
WebEx Access Anywhere

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.

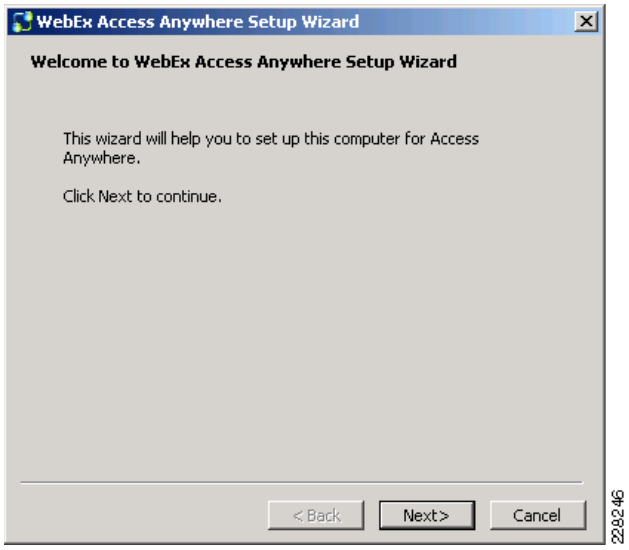
Select **My WebEx** from the tool menu and then click on **My Computers**. See Figure B-174.

Figure B-174



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

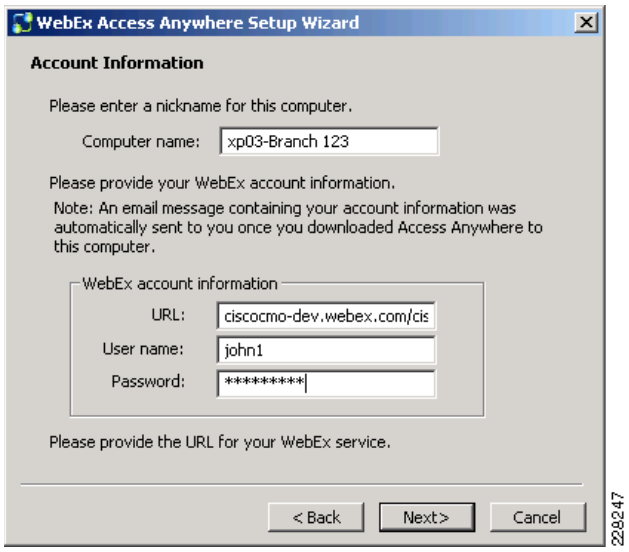
Figure B-175



Step 3 Click **Next**.

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

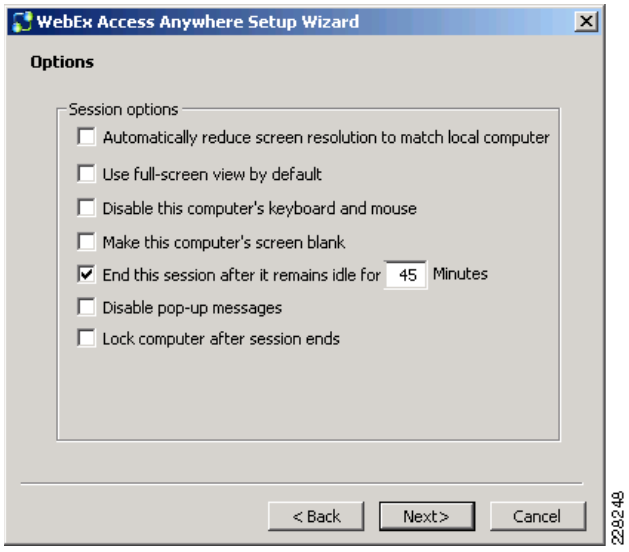
Figure B-176



Step 5 Click **Next**.

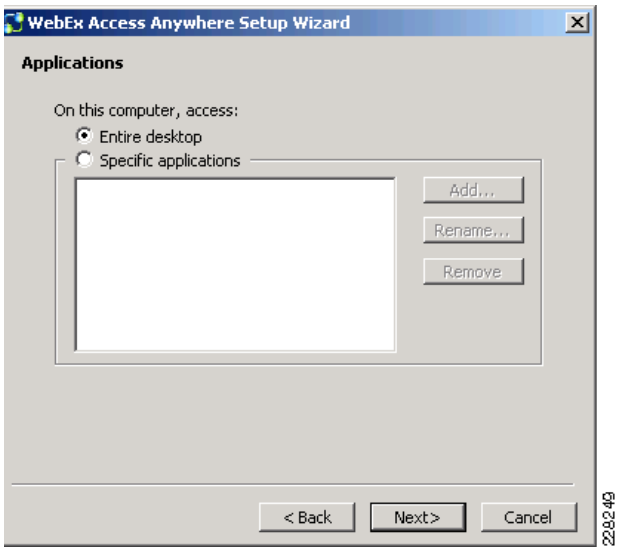
Step 6 For Virtual Expert Kiosks in an Enterprise Branch configure the session options to enable both the Expert and the customer to access and control the System at the same time. Click **Next**. See Figure B-177.

Figure B-177



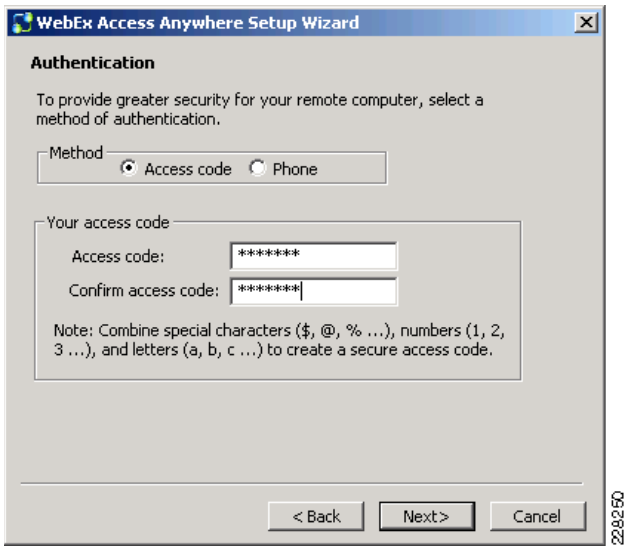
Step 7 Configure access for the entire Desktop and click **Next**. See Figure B-178.

Figure B-178



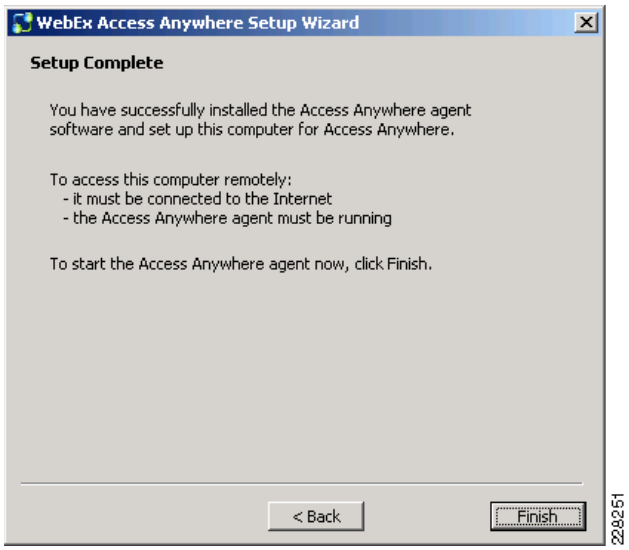
Step 8 Set the Access code for this system and click **Next**.Figure B-179.

Figure B-179



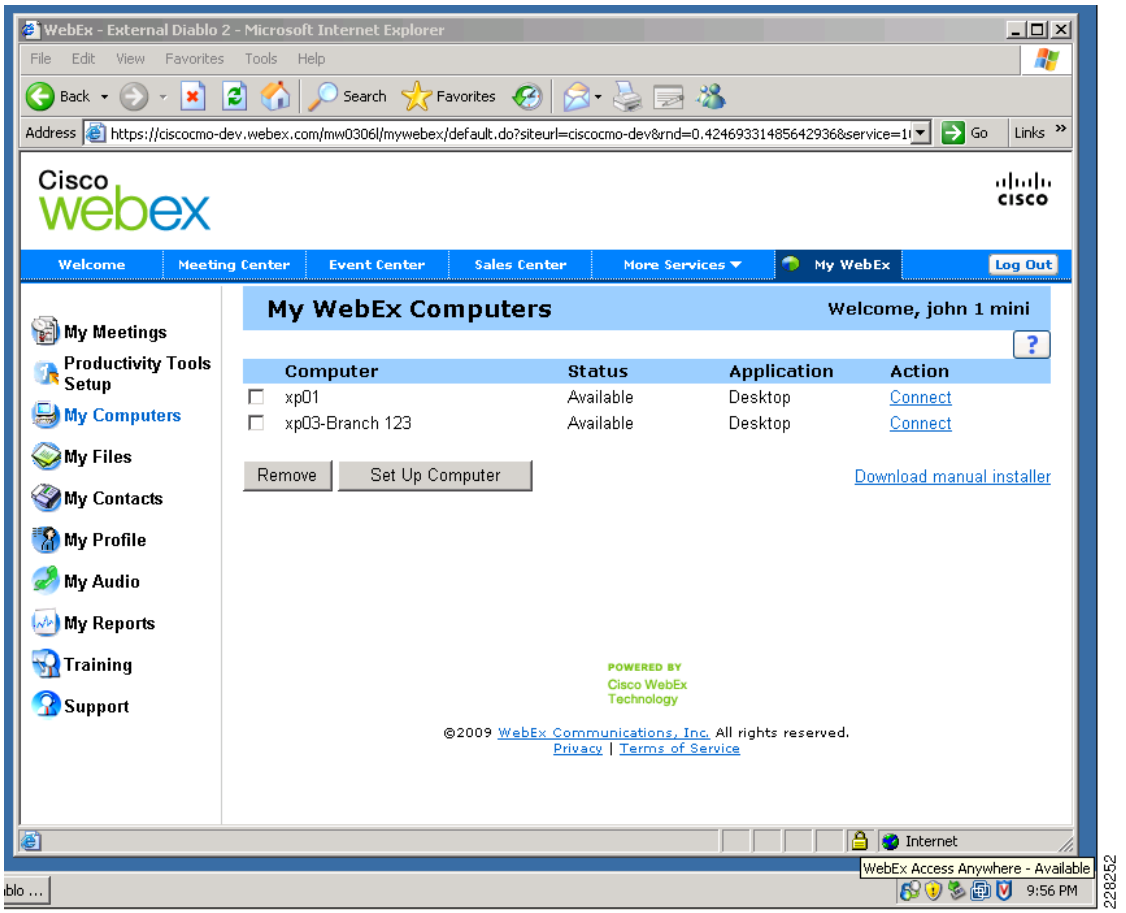
Step 9 With setup completed, click **Finish**. See Figure B-180.

Figure B-180



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-181


WebEx - External Diablo 2 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://ciscocmo-dev.webex.com/mw0306l/mywebex/default.do?siteurl=ciscocmo-dev&rnd=0.42469331485642936&service=1
Go Links
Cisco webex
cisco
Welcome
Meeting Center
Event Center
Sales Center
More Services
My WebEx
Log Out
My Meetings
Productivity Tools Setup
My Computers
My Files
My Contacts
My Profile
My Audio
My Reports
Training
Support
My WebEx Computers
Welcome, john 1 mini
Computer
Status
Application
Action
xp01
Available
Desktop
Connect
xp03-Branch 123
Available
Desktop
Connect
Remove
Set Up Computer
Download manual installer
POWERED BY
Cisco WebEx Technology
©2009 WebEx Communications, Inc. All rights reserved.
Privacy | Terms of Service
Internet
WebEx Access Anywhere - Available
9:56 PM
228252