



Cisco Unified CRM Connector Implementation and Administration Guide for Microsoft CRM, Oracle PeopleSoft and Salesforce.com

Release 1.0

February 2008

Corporate Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100



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

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

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

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

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

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0708R)

Cisco Unified CRM Connector Implementation and Administration Guide
Copyright © 2008, Cisco Systems, Inc.
All rights reserved

Table Of Contents

| | |
|--|----------|
| Cisco Unified CRM Connector Implementation and Administration Guide for Microsoft CRM, Oracle PeopleSoft and Salesforce.com | 1 |
|--|----------|

| | |
|--------------------------|----------|
| Release 1.0 | 1 |
|--------------------------|----------|

| | |
|--------------------------|----------|
| 1. Overview | 3 |
|--------------------------|----------|

| | |
|----------------------|----------|
| Purpose | 3 |
|----------------------|----------|

| | |
|-------------------------------------|----------|
| What Is CRM Connector? | 3 |
|-------------------------------------|----------|

| | |
|---|----------|
| Key Contact Center Concepts..... | 4 |
|---|----------|

| | |
|---------------------------------|---|
| What is a Contact Center? | 4 |
|---------------------------------|---|

| | |
|--|---|
| What are the elements of a contact center? | 5 |
|--|---|

| | |
|--|---|
| What Business Functions does the Contact Center perform? | 6 |
|--|---|

| | |
|--|----------|
| 2. Implementation Planning and Requirements | 7 |
|--|----------|

| | |
|----------------------|----------|
| Purpose | 7 |
|----------------------|----------|

| | |
|---|----------|
| Identifying CRM Connector Components and Installers..... | 7 |
|---|----------|

| | |
|--|----------|
| Cisco CRM Connector Installers..... | 9 |
|--|----------|

| | |
|--------------------------------------|----------|
| Deployment Requirements | 9 |
|--------------------------------------|----------|

| | |
|--|---|
| Deploy a site as a single CRM Connector Server | 9 |
|--|---|

| | |
|--|----|
| Deploy an application connection. | 10 |
|--|----|

| | |
|--|----|
| Deploy for large contact centers. | 11 |
|--|----|

| | |
|------------------------------------|-----------|
| Hardware Requirements | 11 |
|------------------------------------|-----------|

| | |
|---|-----------|
| Operating Environment and Software Requirements..... | 11 |
|---|-----------|

| | |
|--|-----------|
| User Account Requirements | 13 |
|--|-----------|

| | |
|---------------------------------------|-----------|
| Deployment Considerations..... | 14 |
|---------------------------------------|-----------|

| | |
|---|-----------|
| Test Environment Deployment Considerations | 14 |
|---|-----------|

| | |
|--|----|
| Configuring for the Application CTI Server test environment..... | 14 |
|--|----|

| | |
|--|----|
| Configuring for a contact channel test environment | 15 |
|--|----|

| | |
|---|----|
| Hardware Considerations for test servers..... | 15 |
|---|----|

| | |
|---------------------------|----|
| The Test Environment..... | 15 |
|---------------------------|----|

| | |
|--------------------------------------|-----------|
| Implementation Approach | 15 |
|--------------------------------------|-----------|

| | |
|---|----|
| Implementation Steps (and their Order)..... | 16 |
|---|----|

| | |
|---|-----------|
| 3. Implementing the CRM Connector Server | 18 |
| Purpose | 18 |
| Roles, Skills and Resource Required | 18 |
| Before you begin | 21 |
| Install Pre-Requisite Software..... | 21 |
| Install CRM Connector Server Software | 26 |
| What is Installed? | 33 |
| Post Install Steps..... | 35 |
| Configuring Core Modules for CRM Connector Server | 41 |
| Global Section..... | 44 |
| Module Manager Section | 45 |
| Work Manager Section..... | 47 |
| Data Store Section | 47 |
| Event Manager Section..... | 50 |
| Standardized Interface Section..... | 50 |
| CMGateway Section | 51 |
| Remoting Endpoint Section | 51 |
| Soap Module Section | 51 |
| License Manager Section | 51 |
| Configuring the Null CTI Connector for Testing. | 52 |
| 4. Implementing the Administration Tool..... | 54 |
| Purpose | 54 |
| Before you begin | 54 |
| Overview: Administration Tool Features and Functions | 54 |
| Overview: Planning and Deploying the Administration Tool..... | 55 |
| Installation Pre-Requisites | 55 |
| Installing the Administration Tool | 56 |
| Configuring the Administration Tool..... | 65 |
| Configuring the CRM Connector Server for the Administration Tool.... | 68 |
| Administration Tool Section | 68 |
| Using the Administration Tool Implementation | 69 |
| Accessing and logging into the Administration Tool | 69 |
| Registering a New User | 71 |
| Granting User Rights..... | 71 |
| Adding a CRM Connector Server | 73 |

| | |
|--|------------|
| Monitoring and Controlling Server Status | 75 |
| Licensing a Server | 76 |
| Managing Configuration File | 80 |
| Working with Configuration Backups | 81 |
| Editing a Backup File | 82 |
| Managing Logging..... | 83 |
| 5. Implementing the CRM Connector..... | 88 |
| Purpose | 88 |
| Before you begin | 88 |
| Installing the CRM Connector Software..... | 88 |
| Configuring the CRM Connector for Unified Contact Center | 91 |
| Configuring CRM Connector for UICM..... | 92 |
| Confirming the CRM Connector Configuration | 96 |
| 6. Implementing the .NET Adapter | 99 |
| Module Manager Keys | 100 |
| Remoting Endpoint Section | 101 |
| Soap Adapter Section | 102 |
| 7. Implementing the Salesforce.com Adapter..... | 103 |
| Purpose | 103 |
| Overview: Implementation Process Steps..... | 103 |
| Pre-Installation Requirements..... | 104 |
| Installing Salesforce.com Software..... | 104 |
| Configuring the Salesforce.com Adapter | 110 |
| Quick Summary..... | 110 |
| Configure and License the .Net Adapter for .Net Remoting | 110 |
| Import the Call Center Configuration | 110 |
| Edit your Call Center Configuration | 113 |
| Setting for Reason Codes | 116 |
| List of Reason Codes..... | 117 |
| Create, Configure and Assign Agents for the Call Center | 118 |
| 8. Implementing the Oracle PeopleSoft Adapter | 120 |
| Purpose | 120 |
| Overview: Implementation Process Steps..... | 120 |

| | |
|---|------------|
| Pre-Installation Requirements..... | 121 |
| Pre-Installation CRM Connector Steps | 121 |
| Pre-Installation Oracle PeopleSoft Steps..... | 122 |
| Before You Begin..... | 122 |
| Configuring Oracle PeopleSoft Multi-Channel Framework..... | 122 |
| Log In as PeopleSoft Administrator and Navigate to PeopleTools..... | 123 |
| Create a REN Server Configuration..... | 124 |
| Create a REN Server Cluster and test the REN Server | 126 |
| Configure the Multi-Channel Framework Components..... | 128 |
| Configure agents and assign them to queues and configurations..... | 132 |
| Installing the Cisco Application Adapter for Oracle PeopleSoft | 134 |
| Configuring the Cisco CRM Adapter for Oracle PeopleSoft | 143 |
| 9. Implementing the Microsoft CRM Adapter | 146 |
| Purpose | 146 |
| Overview: Implementation Process Steps..... | 146 |
| Pre-Installation Requirements..... | 147 |
| What you will need | 147 |
| Supported Operating Systems and Environments..... | 147 |
| Pre-installation steps..... | 148 |
| Installing the CRM Adapter for Microsoft CRM 3.0 | 148 |
| Configuring the CRM Adapter for Microsoft CRM 3.0..... | 159 |
| Quick Summary..... | 159 |
| Configure Web Service Access | 160 |
| Configure Cisco Contact Center web settings. | 164 |
| Configure Cisco Contact Center global and agent settings..... | 165 |
| Cisco Contact Center Administration Overview | 165 |
| Introduction | 165 |
| Before you begin | 166 |
| Accessing the Administration Pages | 166 |
| Configuring Global Settings..... | 170 |
| Overview | 170 |
| Favorites | 170 |
| Reason Codes | 172 |
| Queues..... | 173 |
| Configuring Agent Specific Settings..... | 176 |
| Overview | 176 |
| Agent Extension | 176 |
| Queue Assignment..... | 177 |
| Channel ID Assignment | 177 |

| | |
|--|-----|
| Agent ACD Credentials | 178 |
| Screen Pop Criteria and Search Order | 178 |
| Set the Auto-Clear On Ready. | 179 |
| Set the Recent Contact Size..... | 179 |

Preface

Purpose

This manual describes how to install, configure and administer Cisco CRM Connector components for Unified ICM and Unified Contact Center Enterprise and Hosted editions. It includes information about hardware and software requirements and setup.

Audience

This book is intended for anyone installing or managing components of the CRM Connector to integrate their contact channels. Installers should be familiar with software installation procedures and the Microsoft Windows Server 2003 operating system. Administrators should be familiar with call center operations and with both the operation and administration of Cisco ICM, UCCE or UCCH, as well as specific implemented CRM business applications: Microsoft CRM, Oracle PeopleSoft, or Salesforce.

Organization

This manual is organized into two parts:

Part 1: Overview, Concepts and Architecture. This describes the role of the CRM Connector software in the integrated contact center, its component products, their architecture and function. This part has two (2) chapters:

Chapter 1: Overview, describes the software and its role in Cisco's Unified ICM and UCCE and UCCH product families.

Chapter 2: Implementation Planning and Requirements, describes the core hardware and software requirements and provides an overview of the installation process.

Part 2: Implementation. This details the software and hardware requirements and installation steps for each major component. This part has seven (7) chapters:

Chapter 3: Implementing the CRM Connector Server, describes step-by-step installation instructions and explains configuration of the CRM Connector Server.

Chapter 4: Implementing the Administrator, describes step-by-step how to install the CRM Connector Server Administration Tool.

Chapter 5: Installing the CRM Connector, describes step-by-step how to install and validate installation of the CRM Connector for Unified ICM and Unified Contact Center Enterprise and Hosted.

Chapter 6: Implementing the .Net Adapter, describes step-by-step how to configure the .Net Adapter. This adapter serves as the

communication enabling foundation for all CRM specific application adapters.

Chapter 7: Implementing the Salesforce.com Adapter, describes step-by-step how to install, configure and validate installation of the Salesforce.com adapter.

Chapter 8: Implementing the Oracle PeopleSoft Adapter, describes step-by-step how to install and configure and validate installation of the Oracle PeopleSoft adapter.

Chapter 9: Implementing the Microsoft CRM 3.0 Adapter, describes step-by-step how to install, configure and validate installation of the Microsoft CRM adapter.

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

1. OVERVIEW

Purpose

This chapter provides an overview of the Unified CRM Connector:

- Its role in the contact center integrating Cisco Unified call management services with contact center business applications;
- Contact Center concepts and terms;
- Its components and architecture.

This manual assumes that readers are familiar with contact center concepts and operations, CTI software and its integration functions and business applications.

Further explanation is available from the Cisco ICM Software CTI Product Description. That manual provides an overview of CTI as well as a description of the Cisco CTI Server, a pre-requisite for the CRM Connector software.

What Is CRM Connector?

The Unified CRM Connector is a CTI application that integrates business applications with contact center channels managed by Cisco Unified Intelligent Call Manager (ICM) or Cisco Unified Contact Center (UCC) Enterprise and Hosted editions.

This integration creates a unified, end-to-end call and business flow from origination in the PBX to hang up and a completed interaction in the business application. It allows contact center agents to manage their ACD work state and their telephone calls within a business application. It also enables a business application “screen pop,” which uses call information to launch the appropriate business form or web page populated with customer contact and other business information.

Integration provides a number of advantages and efficiencies for contact center operations:

1. It simplifies the agent’s environment. Agents are able to perform all their work and contact actions within their business application, using its native features and functions. This frees them from using the special buttons and codes of their telephone device (the phone).
2. It coordinates interaction navigation within one business application window. Agents need not resort to a soft phone window outside their business application. This allows agents to perform customer business transactions and manage their customer phone call within a unified business application interface. It keeps the agents focused on their customer and on application work.

3. It streamlines call handling with contextual call control to help guide agents. They only see the possible call actions and information appropriate for their current call and work state. For example, when a call is “alerting” (ringing), agents only have options to answer or deflect the call; or, when a call is on hold, agents only have the choice of retrieving it from hold.
4. It associates call times and actions with application activities. This allows applications to maintain a customer interaction history, helps develop a more complete picture of agent performance, and enables contact center data warehouse applications to measure overall contact center performance and help identify operational patterns and improvements.

As a supported Cisco product, CRM Connector offers several additional benefits. It provides a stable and validated integration of CRM business applications from major vendors with Cisco’s UICM and UCC contact channel management infrastructure. There is an upgrade path to maintain the integration with new releases of both Cisco Unity products and business applications. Customers are supported by and receive patches and updates through Cisco TAC and standard web support.

Key Contact Center Concepts

Before proceeding it is useful to have a clear, shared understanding of some key contact center concepts and terms.

What is a Contact Center?

A contact center is any business operational unit, large or small, that combines communication channels such as telephone calls, e-mail and web collaboration with business application flows, objects or information to provide business services.

One way to think of a contact center is as another entry way or access point for a business. Similar to retail outlets, field sales and service agents, and web self-service applications, contact centers provide agent assisted services to further sales, customer support and employee helpdesk functions, among others.

Contact centers may be large sophisticated operations or they may be small, departmental units. Call centers supported by UICM or UCC will usually be large and sophisticated, but businesses may have many different sized contact centers, and they may implement contact center functions in smaller departments upon a hosted or enterprise UICM or UCC implementation.

One consistency of a contact center is that it services contact channels, helps manage individual contacts, and involves a business application that applies business processes and involves customer and other business information. Contact centers provide agent assistance, although the agent may be a live human or an automated service such as an IVR.

Integrating the contact channel components with application business objects and data benefits a contact center. Integrated business information

can add call routing information, such as digits entered into an auto attendant that prompts for a customer's service request number, to route the contact to the assigned agent. It may also be used to provide self-service through an IVR: this combines business application logic and flows with the IVR's contact management and prompting functions.

What are the elements of a contact center?

There are four major elements to the contact center:

- **The contact channel infrastructure.** This handles, queues, and distributes phone calls and allows agents to perform call control. In the Cisco environment it consists of a switching platform, either a legacy PBX or Call Manager, ACD skills based routing services provided by UICM (for legacy PBXs), or by UCC for Call Manager, agent phones (call handling devices), either telesets or softphones, and call queuing and voice applications provided by IVRs such as Customer Voice Portal (CVP).
- **The business application infrastructure.** This manages business information and objects, effects business processes and work flows, and performs customer transactions. Common business applications for contact centers are often customer relationship management (CRM) applications such as sales and service offered by major vendors such as Microsoft, Oracle, and Salesforce.com.
- **Communication Contacts or, simply, contacts.** These are usually phone calls but they may also include e-mails, web collaboration and chat sessions. There are three parts to a contact, they may be treated and tracked as a unit or each may be used separately:
 - **Streaming Media or contact media: this is the communication content** -- for phone calls this is the voice conversation, for e-mail it is the e-mail body, and for web chat it is the exchange between agent and customer.
 - **Contact metadata.** This is information about the contact media such as the e-mail header or the call network or switch information, e.g., ANI, DNIS, etc.
 - **Contact context information.** This is additional content information, such as call attached data. This includes customer entered digits from an IVR or additional information such as Service Request number or thread information parsed from an e-mail, etc. It adds context or meaning to the interaction outside the channel state and data.
- **Agents.** Agents may be people, "live agents," or automated agents such as IVR self-service applications. There are two classes of live agents:
 - Full service or "heads down" agents are contact center agents who log into ACDs or outbound campaigns to receive continuous work distributed from a queue or list. Most Tier 1 service agents, help desk agents, and internal sales agents are full service workers.

- Knowledge workers who work independently but have contact communications and work in business applications. They may select their next action and work outside of the contact center.

Although the Cisco CRM Connector only supports full service, ACD agents, knowledge workers can use this system: they must be configured for and log into the UCC or UICM integrated ACD, but they need not receive calls through a queue.

IMPORTANT WARNING: You must configure a queue in the CRM application adapter settings. You **must assign** a queue to each call center agent, even if you do not use queues (or skills) in UCC or the ICM integrated ACD. You may assign a “phantom” queue value, such as 1, 10 or 9999. Agents will not be able to log in without this queue assignment.

What Business Functions does the Contact Center perform?

Most contact centers perform customer relationship management (CRM) and the integrated business applications are CRM applications. Broadly, CRM applications provide sales and customer service functions including standard support and case management software, help desk functions for both technical and employee help desks, marketing campaign execution and management and financial help desk functions such as collections and payment assistance.

CRM applications manage several high-level lines of business relationships, but the most common include:

- Business to Business (B2B), for example sales and service for major software or business services.
- Business to Consumer (B2C), direct support for consumer retail sales or service.
- Business to Employee, for example IT technical support and HR employee help desks.
- Government to Citizen (G2C), this includes governmental services support for 311 and 211 functions.
- Partner to Partner, as the name implies this manages a partnership relationship.

Many businesses have several contact centers to support different lines of business relationships and provide different functional services, such as sales and customer support.

2. IMPLEMENTATION PLANNING AND REQUIREMENTS

Purpose

Definition: Implementation is the process of installing, configuring and stabilizing CRM Connector product components.

This important chapter describes the implementation process. It explains important concepts and has substantial information about the requirements, installation steps, configuration and validation of a successful Cisco CRM Connector implementation.

You should read this chapter.

Read this chapter as part of the contact center project planning phase. This will help you:

- identify which product components must be installed to support your contact center;
- determine the appropriate deployment strategy for your contact center components;
- understand the hardware, software and network pre-requisites of the contact center;
- understand the implementation process steps;
- identify the next implementation chapters you must read to implement your specific product components.

Identifying CRM Connector Components and Installers

The Cisco CRM Connector is a set of component products. Each component performs specialized functions and must be installed, configured and validated separately.

This section helps you identify which product components support your contact center, which installers to use, and which implementation and administration chapters you will need to read.

The main components of the Cisco CRM Connector are

- **The CRM Connector Server. You must implement this core component.** It is the core integration engine. It provides general services, manages agents, communication channels and individual contact (phone call) states; it normalizes events, information and commands. Read Chapter 3: *Implementing CRM Connector Server*; use the CRM Connector Server installer.
- **The CRM Connector Administration Tool. You should implement this component.** It allows you to manage your CRM

Connector components, change configurations, monitor and control the CRM Connector Server, and to monitor your agents' work states. Without this tool, configuration and administration of the CRM Connector is significantly more difficult. Read Chapter 4: *Implementing the Administration Tool*; install using the CRM Connector Server Administration Tool installer.

- **The CRM Connector for Unified ICM and Unified Contact Center Enterprise and Hosted. You must implement this component.** It connects with CTI Server to integrate the Cisco contact center channel. Read Chapter 5: *Implementing the CRM Connector*; use the CRM Connector Server installer to install the CRM Connector.
- **A CRM Adapter. You must implement at least one CRM Adapter.** CRM adapters integrate business applications with the contact center. You may implement more than one CRM Adapter if you use multiple applications, for example both Oracle PeopleSoft and Microsoft CRM to support two different organizations. The implementation and deployment of the CRM Adapter is driven by the end-application's channel integration infrastructure. Most adapters integrate with a server-level application integration framework however a few, such as the Salesforce adapter, require deployment of desktop components.

Cisco supplies the following business application adapters:

- **Salesforce.com Adapter.** Install this adapter if you subscribe to Salesforce.com Call Center Edition, which is an add-on component of the Customer Service and Support module for the Professional, Enterprise and Unlimited editions of Salesforce. The Salesforce integration framework architecture requires deploying components to the agent's desktop. Read Chapter 7: *Implementing the Salesforce.com Adapter* and use the CRM Adapter for Salesforce.com installer.
- **Oracle PeopleSoft Adapter.** Install this adapter to integrate PeopleSoft 8.9 or higher. This adapter requires PeopleTools 8.45 or higher. Cisco recommends customers implement PeopleTools 8.47 or higher. Read Chapter 8: *Implementing the Oracle PeopleSoft Adapter*; use the CRM Adapter for Oracle PeopleSoft installer.
- **Microsoft CRM Adapter.** Install this adapter to integrate Microsoft's CRM product. Unlike other applications vendors, Microsoft does not provide a Contact Center integration framework. The adapter extends the MS CRM, adding an integration framework, administration utilities, and contact center user interface with a channel controller. Read Chapter 9: *Implementing the Microsoft CRM Adapter*; use the CRM Adapter for Microsoft CRM 3.0 installer.

Cisco CRM Connector Installers

There are six installation programs. There is a single installer for the core components: the CRM Connector Server and the CRM Connector for Unified ICM and Unified Contact Center Hosted and Enterprise. There are separate installers for the CRM Connector Administration Tool and one for each CRM Adapter.

Table 2-1: Installation Selection List

| Installation Program Name | Product Components Installed | Reference Chapter(s) | Required | Install |
|--|---|----------------------|-------------|---------|
| CRM Connector Server Installer | CRM Connector Server | Chapter 3 | REQUIRED | Yes |
| | CRM Connector for Unified ICM and Unified Contact Center Enterprise and Hosted. | Chapter 5 | REQUIRED | Yes |
| | CRM .Net Adapter | Chapter 6 | REQUIRED | Yes |
| CRM Connector Server Administration Tool Installer | CRM Connector Server Administration Tool | Chapter 4 | RECOMMENDED | Yes |
| CRM Adapter for Salesforce.com Installer | CRM Adapter for Salesforce.com | Chapter 7 | Optional | |
| CRM Adapter for Oracle PeopleSoft Installer | CRM Adapter for Oracle PeopleSoft | Chapter 8 | Optional | |
| CRM Adapter for Microsoft CRM Installer | CRM Adapter for Microsoft CRM | Chapter 9 | Optional | |

Table 2-1: Installation Selection List lists the installers, the installed product component and the chapter in this implementation guide that explains how to implement each component. It also identifies whether the component is optional or required.

Deployment Requirements

Definition: A site is a simplex or duplexed peripheral device monitored through a CTI Server connection for a single Unified ICM or Unified Contact Center implementation.

Deploy a site as a single CRM Connector Server

The definition of site above has important implications to the deployment and configuration of the Cisco CRM Connector.

A site equates to a single peripheral or “switch.” That is, there is one site for each peripheral interface manager (PIM) associated with a peripheral gateway (PG). The Cisco CRM Connector uses the peripheral id (PID) to maintain a logical connection through the CTI Server with each peripheral switch.

A site therefore is not limited to a single geographic location or organizational unit. It is any set of agents serviced by the same PBX. For Unified Contact Center configurations there is only one PID for the enterprise gateway and therefore one site. However for legacy switches there can be up to 32 peripheral interface managers per PG.

The CRM Connector configures connections with switches through “CTI Modules”. Each configured CTI module has a unique name on its CTI Connector Server and is associated with a specific peripheral type and assigned to a specific peripheral ID.

Put simply: site = CTI Module configuration = PID = switch.

A single CRM Connector Server may support one or more CTI Modules and therefore multiple sites. Most customers deploy one CRM Connector Server for each site. There are a number of advantages for this, primarily it reduces the risk if a single server fails, isolating the outage to a single site.

You may wish to configure sites based on organizational units or geographic locations, even if they are served by the same peripheral. This is a valid deployment. Since the site name is often configured within the business application it can be useful for reporting purposes. However this can make administration more difficult, even if there is only one CRM Connector Server. In general it is better to treat a single switch configuration as a single site and rely on agents, and groups or skills to resolve sites for reporting purposes.

Deploy an application connection.

Definition: Application CTI communication server: the communication infrastructure for a CRM business application.

Each CRM business application provides its own CTI integration architecture. With few exceptions, e.g. Salesforce, these are server level integrations that connect through an application CTI communication server. CRM Connector integrates with CRM applications through an application adapter. The application adapter maintains a single logical connection with the application CTI communication server.

You will only need to configure one application adapter connection for each application instance. Most CRM applications are configured for a single instance; this ensures a central, single source of truth about customers, products and service processes and procedures.

Multiple CRM Connector Servers can be configured for a single business application instance. Therefore if you deploy a multi-site, multi-server configuration, each will be able to connect through the application CTI communications server.

Applications scale their communication services through different mechanisms including server clusters or multiple communication servers. These may require additional configuration for the application, but not on the Cisco CRM application adapter.

Deploy for large contact centers.

In general it is best to have one CRM Connector Server for each site. A single CRM Connector Server can support 1800 end users (agents). Therefore very large sites, such as an Enterprise UCC site, may require multiple CRM Connector Servers.

Hardware Requirements

Exact system requirements depend upon the number of simultaneous users. The CRM Connector Server is highly scalable and able to support very large numbers of users.

A single CRM Connector Server can support up to 1,800 agents using the configuration below. Additional agents can be supported by deploying multiple CRM Connector Server configurations. Smaller sites may consider installing the CRM Connector Server on CRM application servers. Check with your application vendor to be sure they support co-resident services. Cisco does **not** support co-residing CRM Connector Server on PG servers. Cisco does not support implementing CRM Connector Server production instances on virtual servers or virtual machines.

Table 2-2: Hardware Requirements for 1800 Agents

| Component | Minimum Requirement |
|--------------------|---|
| Processors (CPU) | 4 dual-core, hyper-threaded CPUs |
| Memory | 8GB RAM |
| Disk Storage | 2GB consumed |
| Network Connection | IP connection, 1GHz Ethernet Connection |

Table 2-2: Hardware Requirements for 1800 Agents shows the certified hardware requirements for a large site. As noted, larger sites will require additional instances of the CRM Connector Server.

Operating Environment and Software Requirements

The Cisco CRM Connector is built upon a Microsoft operating environment infrastructure. All components are built using Microsoft's development tools and are designed to run on a Windows 2003 Server. Components communicate through a number of Microsoft technologies including DCOM and .NET.

Table 2-3: Operating Environment Infrastructure

| Software Component | Use and Notes |
|----------------------------------|--|
| Microsoft Server 2003 SP1 or SP2 | Primary operating system. If there is any delay in Cisco validating a Microsoft patch, you may safely apply regular Microsoft required patches so long as you test them in your test / development |

| Software Component | Use and Notes |
|---|---|
| | environment first. |
| Microsoft .NET Framework V2.0 | Application adapters use .NET remoting and .NET web services for communication. The Administration Tool uses .NET web services to communicate with and manage CRM Connector Servers. |
| Microsoft Message Queuing Services (MSMQS) | Message queuing distributes events across web services components. |
| Microsoft Internet Information Server (IIS) | Microsoft IIS allows execution across web services components. |
| DCOM | Microsoft DCOM must be configured to support CRM Connector Server inter-module communications. Each CRM component module is a DCOM component. |
| ASP.NET 2.0 | This is a Microsoft IIS configuration. You must enable IIS for ASP.NET, which is used by web services. NOTE: If you install .NET V2.0 before you install IIS you may need to run <i>aspnet_regiis.exe</i> to map properly the ASP.NET version 2.0 scripts with IIS. |
| Microsoft Windows Domain | A Microsoft Windows domain is supported, but not required. If you have multiple CRM Connector servers this may help you configure users and security. You may use the domain configured for your Cisco Unified ICM or Unified Contact Center implementation. Note: a domain account is required for certain distributed configurations of the Administration Tool. |
| Microsoft SQL Server | This is required for the Administration tool. If your organization does not use Microsoft SQL Server you may install Microsoft SQL Server Express 2005. This can be obtained and used without license fees from Microsoft's development site. |

Some application adapters require deploying components on the agent desktop. These special requirements are documented as part of the application adapter's implementation chapter. Follow your CRM application vendor's requirements for the agent desktop working environment: the OS, the browser, etc.

Server based application adapters must be deployed on the application communication CTI server. For these adapters, you must deploy the application communication server on a Windows platform. Many organizations deploy application services on Linux and other operating systems. This is supported through remote connections such as .NET

remoting and .NET SOAP interfaces. However, when the adapter runs within an application communication server's process, you must deploy the application communication server on a Windows platform.

Some application adapters run in a Java machine and require a Java runtime environment, e.g., PeopleSoft. The Cisco Unified CRM Connector requires these Java based components run on a windows server machine. You will need to install the appropriate windows Java runtime. This requirement is documented in the application adapter implementation chapter.

User Account Requirements

You will need to configure Windows, application and ACD users for your implementation. The Window's operating system user will need local administration rights on the CRM Connector Server and be must configured with administration privileges for Microsoft IIS and as well as some DCOM and .NET functions. You may wish to use a special domain account to simplify administration, this does not need to be a domain administrator but the user must be included in the local administrators group on all servers running Cisco CRM Connector Server components.

Table 2-4: User Accounts for CRM Connector

| Account Type | Use and Configuration Considerations |
|---------------------------------------|--|
| Windows domain account | Administer Cisco CRM Connector Servers Add this account to the local administrators group for all running Cisco CRM Connector product components. |
| Windows agent account | For applications with application adapter components deployed on the agent desktop, each agent will need to run windows and have a local (or domain) account. |
| ACD agent logins | Agents must log into the ACD, each agent, test or production, in your environment will need an ACD login. Note, applications support single sign-in; you will need to configure the agent's ACD login information (agent ID and password) in the application CTI framework. |
| Application login | Agents must be able to log into the business application. Each agent requires a unique login. |
| MS SQL Server DB administrator login. | You should have a system administrator login to the MS SQL Server (or SQL Server Express) instances. This will allow you to create the appropriate databases and users necessary for the Cisco CRM Connector Server Administration Tool. |

Deployment Considerations

The Unified CRM Connector Server's component architecture opens a number of deployment options for complex enterprise contact center implementations. When considering implementation requirements there are three (3) significant, basic deployment strategies that need to be addressed:

- The single instance, single site contact center.
- The large enterprise, distributed contact center.
- The multi-site contact center. There are three categories of multi-site contact center:
 - 1) the organizational site; this defines a site as an organizational unit that is segregated for accounting, performance metrics or other operational or administrative reasons;
 - 2) the geographic site; this defines a site as a geographic location;
 - 3) the switch based site; this defines a site as a single switch (PBX).

Test Environment Deployment Considerations

Every implementation must include a test CRM Connector Server instance and should also include development and training instance configurations. These can be handled by one or several separate CRM Connector Servers configured for dedicated test, development, and training application and contact channel environments. This parallels the staging for application implementation and support strategies for CRM and ERP business applications.

Configuring for the Application CTI Server test environment

Most organizations have dedicated test and development instances of their business application. This usually requires separate application communication CTI servers for each environment.

Configure the CRM Connector test environment application adapter to connect with the test application CTI communication server. Often a single combined test / development CRM Connector Server will support both test and development environments. As needed, using administration tools you can configure the application adapters for specific test and development application instances.

This implementation protects the integrity of production application data.

Configuring for a contact channel test environment

Organizations rarely implement dedicated test and development PBX and other channel hardware instances. Instead dedicated test, development and training configurations are built out on the production platforms with an isolated set of route points, queues, IVR voice scripts and agent phones and ACD logins configured for test, development and other purposes.

This ensures that test, development and training phone calls and agent sessions will not accidentally bleed into the production work. It also protects the integrity of production switch reports.

Hardware Considerations for test servers

Test environments still must meet the minimal hardware requirements, but they can be deployed on virtual servers from VMWare or other VM services that support two or more processors per virtual server.

The Test Environment

The test environment should include a CRM Connector Server with the appropriate connector and adapters installed and configured to point to the test environments.

You should have a test pathway implemented on your switch and within your IVR, with scripts that segregate test agents and phone calls and information from production work.

The telephony test environment should be able to receive and make calls to the public network (PSTN). To simulate the production environment, the test telephony environment should be able to handle and queue multiple calls.

Three agent test configurations are necessary to test conference and transfer scenarios, but also to test multiple calls in the queue. In addition to the properly configured CRM Connector Server configuration you will need three (3) agent desktops consisting of an agent PC, an agent telephone configured with test extensions, logins to test agent ACD skills and queues and a login to the test application environment. Agents should be able to receive queued calls placed from the PSTN and where allowed, be able to place outbound calls through the PSTN. If production agents may receive direct inward dialed calls, then the test environment should also be configured for this feature.

Implementation Approach

Cisco recommends an incremental approach to implementing the CRM Connector components. This approach installs, configures and validates each CRM Connector product component before implementing the next component.

Using this approach you should first implement the pre-requisite software and make sure that the IIS services are working properly and that the .NET components work in your environment.

You will need to perform complete, independent implementations, one for the test / development environment and a second for the production environment.

Implementation Steps (and their Order)

Install and configure operating environment pre-requisites.

- Install Windows Server 2003
- Install .NET Framework V2.0
- Install and configure application server components for Windows Server 2003
 - IIS
 - ASP.NET
 - Message Queuing
- Test and validate the IIS and .NET Framework configuration.

Install CRM Connector Server and configure with the test “null” connector.

- Install the CRM Connector Server.
- Perform all post-install windows operating environment configurations to support DCOM and .NET web services.
- Perform post-install IIS configurations.
- Create the CRM Connector config.ini file configured with the test “null” connector.
- Start the CRM Connector Server; ensure that all of the logs show proper startup.

Install the CRM Connector for Unified ICM and Unified Contact Center Enterprise and Hosted.

- Before installing, use Cisco tools to verify connection and configuration of the CTI Server and peripherals that you will connect with.
- The CRM Connector software is installed as part of the CRM Connector Server installation.
- Replace the test “null connector” CTI Module configuration with the proper Cisco CTI Server configuration information.
- Re-start CRM Connector Server; ensure proper start up and connection to the CTI Server.
- Log agents into and out of the phones manually and place test calls to queues and directly to the agent extensions to ensure that the calls, queues, events and information are properly monitored and recorded in the log files.

Install and configure application adapters.

- Before installing, use the application's tools to verify connection and configuration of the application CTI communication server and application services.
- Use the appropriate application adapter installer to install the application adapter software.
- Follow the implementation directions to configure the application adapter. Note that most application adapters require two or more separate configuration efforts:
 - Configure the CRM Application adapter in the CRM Connector Server config.ini file.
 - Use the application administration tools to configure the appropriate connectors and settings for the application CTI communication server.
 - Create and assign agents within the business application. This will require setting up each agent's ACD and telephony connection settings as well as assigning them to the correct services.
- Re-start the CRM Connector Server and validate the application adapter connections.
 - Check the log files to make sure the application adapter connection is working.
 - Log the contact center agent into the business application.
 - Use the application services to log the agent into the UICM ACD functions.
 - Place test calls to the agent both through the queues and, if supported, with direct dials.
 - Perform standard inbound and outbound telephony tests to ensure that the agent can log into and out of their ACD account, receive inbound calls (both from queues and through direct dials) and place outbound calls. Test on both the agent teleset (or softphone) and using the application communication toolbar to be sure that the phone and the application communication toolbar stay synchronized.

Many implementers may be tempted to take a “big bang” approach, installing all product components, configuring them and then validating the end-to-end installation. This “big bang” approach should only be taken by experienced systems engineers who are confident the underlying dependent software services are properly configured and operational.

The methodical approach described above may appear more time consuming, however by validating each component's implementation at each step you will save considerable time resolving any problems you might encounter.

3. IMPLEMENTING THE CRM CONNECTOR SERVER

Purpose

This chapter describes the software installation process for the CRM Connector Server. You must install at least one CRM Connector Server and should install one per configured site as noted in *Chapter 2: Implementation Planning and Requirements*

Implementation Planning and Requirements

This chapter covers:

- Roles and skills required to implement the CRM Connector Server.
- Installing and configuring pre-requisite software.
- Installing and Configuring the CRM Connector Server.
- Testing the CRM Connector Server installation.

This section assumes that distributed components, such as IIS, are running locally on the CRM Connector Server machine. This is a rather simple configuration. For large implementations, Cisco recommends a distributed deployment with IIS and any CRM Connector web services installed on a separate machine from the CRM Connector Server.

Roles, Skills and Resource Required

Different people are often responsible for specific implementation tasks. For example, some organizations require that software is installed and patched by the IT group, but the actual administration and configuration of software is the responsibility of local users. In most organizations a single IT or communications person will have multiple software management, implementation and administration roles and skills.

To support the full range of users this section identifies specific roles, their responsibilities and required skills. Each step will identify which user roles are required and which may need to be available to complete the step.

Role: Server Administration

Responsibility: To configure and manage the server system. This person is responsible for ensuring that the hardware is properly configured, the core operating system is installed and operational.

Skills:

- Install and test server class hardware.
- Install and validate core Windows Server 2003 operating system components.

Role: Network Administration

Responsibility: Ensure the CRM Connector Server is properly configured for the network and assigned IP addresses and host names.

Skills:

- General network administration skills.
- General IP network and domain services (DNS).
- Ability to troubleshoot IP network configuration settings.

Role: Windows Administrator

Responsibility: Install and configure windows operating environments, including DCOM and .NET. Create and manage windows user domain and local accounts and privileges.

Skills:

- Manage and configure Windows Server 2003 operating system.
- Create user accounts.
- Establish and enforce Windows system security settings.

Role: Windows Application Administrator

Responsibility: Install and configure windows application services such as IIS, MS Message Queue and server class software.

Skills:

- Install, configure and administer IIS and MS Message Queue.
- Install and configure server software.

Role: Voice Platform Administration

Responsibility: This person is responsible for the administration of the Cisco Unified ICM or Unified Contact Center services. The skills and responsibilities may be assigned to more than one person.

Skills:

- Create and manage agent ACD logins
- Administer CTI Server connection information.
- Administer PG and PIM connection information.
- Use Cisco tools to validate CTI Server connections.
- Provision telesets or softphones.

Role: Application System Administrator

Responsibility: This person is responsible for the administration of the business application, management and configuration of application services.

Skills:

- Manage, configure and debug distributed computing application environments.
- Configure the specific business application.
- Configure and administer the application CTI communication services component – this skill may be learned as part of the contact center implementation process.

Role: Application User Administrator

Responsibility: Configure, provision, and administer application user (agent) logins.

Skills:

- Create and configure application users: assign user access rights, privileges, roles and responsibilities.
- Configure contact center agent user settings within the business application – this skill may be learned as part of the contact center implementation process.

Role: CRM Connector Implementation Coordinator

Responsibility: This person is responsible for coordinating the implementation process and engaging resources as needed, ensures that all implementation steps are followed and unit tests, integration tests and end-to-end system tests are completed.

Skills:

- Capture business requirements and define business processes.
- Works with voice and application systems groups to coordinate configuration information.
- Understand the operation, architecture and implementation processes and procedures for the CRM Connector Server and its components and the application channel integration framework.

Role: CRM Connector Implementer

Responsibility: This person is responsible for installing, configuring and validating the Cisco CRM Connector product set. This person also performs or participates in CRM Connector product component unit and integration tests and participates in the end-to-end system tests.

Skills:

- Understand contact center architecture.
- Understand Cisco Unified ICM and Unified Contact Center Enterprise and Hosted system components and architecture
- Coordinate and work with business application and Cisco voice platform administrators.
- Manage, configure and debug distributed computing application environments.

- Install, configure, and debug Microsoft Windows application software and operating environment enabling software.
- Understands database configuration and installation scripts.

Before you begin

- Read Chapter 2: *Implementation Planning and Requirements*
- Read this chapter.
- Have your CRM Connector Server prepared
 - Windows Server 2003 Operating System with SP1 or SP2 should be installed
 - The server should be connected to the network.
 - Have a Windows domain user account or a local Windows user account. This account must be a member local administrators group for CRM Connector machines.
 - Know and record the following information:
 - Windows administrator user account name and password.
 - Windows server machine name.
 - Windows server machine domain (if used)
 - Windows server machine IP address.
 - Windows server machine host name.
 - Windows IIS configuration information.

Install Pre-Requisite Software

To install the pre-requisite software you must have the CRM Connector Server machine configured with the Windows Server 2003 operating system with SP1 or SP2 and a user account with local system administration privileges.

You may need to install the following software components; they should be installed in this order:

1. Microsoft Windows Server 2003 Service Pack 1 or Service Pack 2 (accessible from Microsoft's web site).
2. Microsoft IIS (included with the operating system distribution).
3. Microsoft Message Queuing Services (included with the operating system distribution).
4. Microsoft .NET Framework V2.0 (accessible from Microsoft's web site).

Note: this is included in the CRM Connector Server installations and can also be installed as part of the CRM Connector Server installation.

5. Microsoft SQL Server Express 2005 (accessible from Microsoft's web site), if installing the Administration Tool.

Note: this is required if your organization does not have or plans not use a production instance of Microsoft SQL Server 2000 or greater. This is required for the Administration Tool and it is useful to install it at this step.

Step 1: Apply Microsoft Windows Server 2003 Service Pack 1 or Service Pack 2.

Windows Server 2003 SP1 is the minimum supported operating system level for Cisco CRM Connector Server. Windows 2003 SP2 is also supported. You will need to verify the version of your operating system and apply the service pack if it is not already applied as well as any current critical patches from Microsoft.

Quick Steps

- **Check the current Windows Server patch level:**
 - **Windows Explorer: Help→About**
 - **Download Windows Server 2003 Service Pack 1 or Service Pack 2 from the Microsoft Download site.**
 - **Apply the Service Pack: follow Microsoft Instructions**
- **Apply latest Windows Updates**
 - **Microsoft Internet Explorer: Tools → Update**
 - **Using the Express option applies all critical patches**

Windows Server 2003 SP1 is the minimum operating system level supported. To identify the implemented operating system version open Windows Explorer and select **Help→About** from the menu bar. This displays the “About Windows” dialog that shows the version, the build, and the Service Pack level. The screen shot below Figure 3-1: About Windows Dialog shows the tested Windows version for SP2:

- Version 5.2
- Build 3790
- Service Pack 2
- At the bottom it also shows the total physical memory available to Windows; your system should have at least 8 GB of memory to support 1800 agents.

Figure 3-1: About Windows Dialog



Step 2: Install Microsoft IIS

Microsoft Internet Information Services is required for a number of application components that rely upon .NET web services.

Quick Steps

- **Log into windows with local administrator account.**
- **Open the Windows Components Wizard**
 - **Start → Control Panel → Add / Remove Programs**
 - **Add/Remove Programs Dialog → Left Menu Bar → Add/Remove Windows Components**
- **Select and apply the following features using the Windows Components Wizard:**
 - **ASP.NET**
 - **Microsoft Internet Information Services**
 - **Microsoft Message Queuing Service**

Before you begin: Microsoft IIS is part of Windows Server 2003: you will need the Windows Server 2003 installation distribution CD. You will also need access to the service pack files.

1. Log into the local Windows system.
2. Use the Control Panel “Add / Remove Software” option to launch the Add or Remove Program Dialog. Select Add / Remove Windows Components (from the left hand menu bar). This launches the Windows Components Wizard.

Start → Add or Remove Programs

Add/Remove Windows Components (left menu side-bar option)

Note: you may also use the Windows Server 2003 installation program, to launch the Windows Components Wizard.

From the wizard select the Application Server option, then press Details to launch the Application Server Dialog:

Click / Select Application Server → Details (button)

3. Check ASP.NET. This enables support for ASP.NET on the IIS server. If you omit this step, you will need to enable ASP.NET manually on your IIS later.
4. Select Internet Information Services (IIS) and press the Details button to select your IIS configuration. This launches the Internet Information Services (IIS) dialog.
5. Verify that by default the following components are checked for installation:
 - Common Files
 - Internet Information Services Manager
 - World Wide Web Service.

Note: The World Wide Web Service has a detail option, by default only the World Wide Web Service is checked and enabled. This is all that is required for this implementation. If you wish you may validate this by selecting World Wide Web Service and the Detail button or simply check the box to install WWW Service.

6. Press OK to complete the Internet Information Services (IIS) dialog.
7. From the Application Server dialog select Message Queuing and press Details to launch the Message Queuing Dialog.
8. By default the “Active Directory Integration” and “Common” options are selected. These are all the required components.
9. Press OK on the Message Queuing dialog to accept the settings; this returns you to the Application Server dialog.
10. Verify that the following options are enabled (checked) on the Application Server dialog:
 - ASP.NET
 - Enable network COM+ access (this should have been enabled on your original installation).
 - Internet Information Services (IIS). [the check box will be grayed and checked because you are not installing all IIS components]
 - Message Queuing [the check box will be grayed and checked because you are not installing all MQ components]
11. Press OK to accept these options and close the Application Server dialog. This will return you to the Windows Components Wizard.
12. Press Next on the Windows Components Wizard, this will install and configure the selected components: ASP.NET, IIS and Message Queuing.
13. When the configuration installation is complete, press “Finish”
14. At this point you should close the Add or Remove Programs Dialog or the Windows Server setup contents dialog and check for

critical Windows updates because there may be patches or updates for the installed components.

15. When the Windows updates are complete, reboot your Windows server.

Step 3: Confirm IIS configuration.

After installing IIS test to be sure that you can open the default pages.

1. On the local server or on a remote machine open an IE browser and enter the IIS server's host name or IP address. This should display the default page: the standard "under construction" message. If this page does not launch or if the site cannot be reached you will need to resolve your IIS installation.

A word of warning: some actions described here and later behave differently on the IIS server machine from how they behave on a remote system. On the local server you may also find that different pages will display when using the host name than using the IP address. Since all connections ultimately will be remote and distributed it is a good idea to test both on the local server box and on a remote workstation.

This documentation will advise if an action can only be performed on the local server.

Step 4: Install Microsoft .NET Framework V2.0.

You may download .NET Framework Version 2.0 Redistributable Package (x86) from the Microsoft Download Site. Install it following Microsoft's directions. You must install .NET Framework if you are also installing SQL Server Express (Step 5).

Note: if you do not install this independently, the CRM Connector Server installer will detect its absence and install it. Therefore this installation step is included in the CRM Connector Server installation directions.

Step 5: Optional – Install MS SQL Server Express – for the Administration Tool.

At this point, if you have installed the .NET Framework V2.0, you may install MS SQL Server 2005 Express if you are not using a production instance of MS SQL Server 2000 (or greater). Microsoft allows businesses to install this to support run time SQL Server applications.

1. As of the date of this document's publication, you may use this link to navigate to the SQL Server 2005 Express web site:
<http://msdn.microsoft.com/vstudio/express/sql/>
2. Follow the directions there to download and install SQL Server 2005 Express. You may also wish to register your copy with Microsoft before downloading the software.
3. Cisco recommends you also install the SQL Server Manager Studio Express. This simplifies administration of SQL Server. You may either download it separately from the Microsoft site or download the Advanced version which includes it. You will not need the Toolkit for this implementation.

4. You should install SQL Server Express in mixed security mode. CRM Connector components use SQL Server authentication in order to support both domain and non-domain Microsoft Windows implementations.

Note: You must install .NET Framework V2.0 first: it is **required** for SQL Server 2005 Express.

This completes the pre-requisite software installation steps.

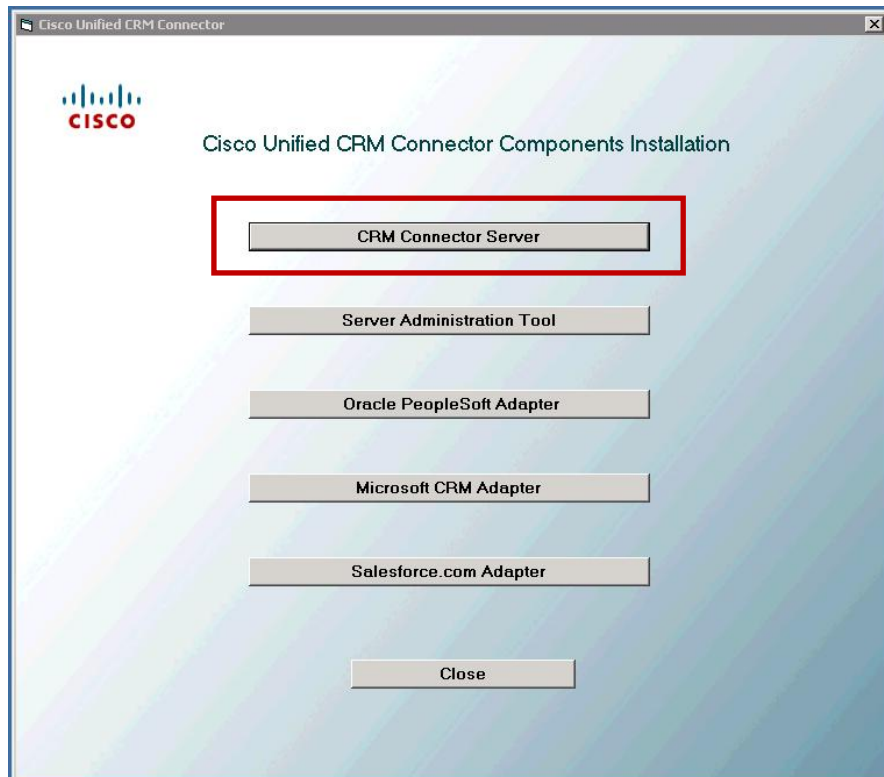
Install CRM Connector Server Software

This section takes you through the install wizard for CRM Connector Server Software. This is very straightforward with only a few options.

Note: If Microsoft .Net Framework V2.0 is not installed on the server the InstallShield wizard will install it automatically.

Step 1: Start the installation and select the Cisco Unified Contact Center Enterprise component.

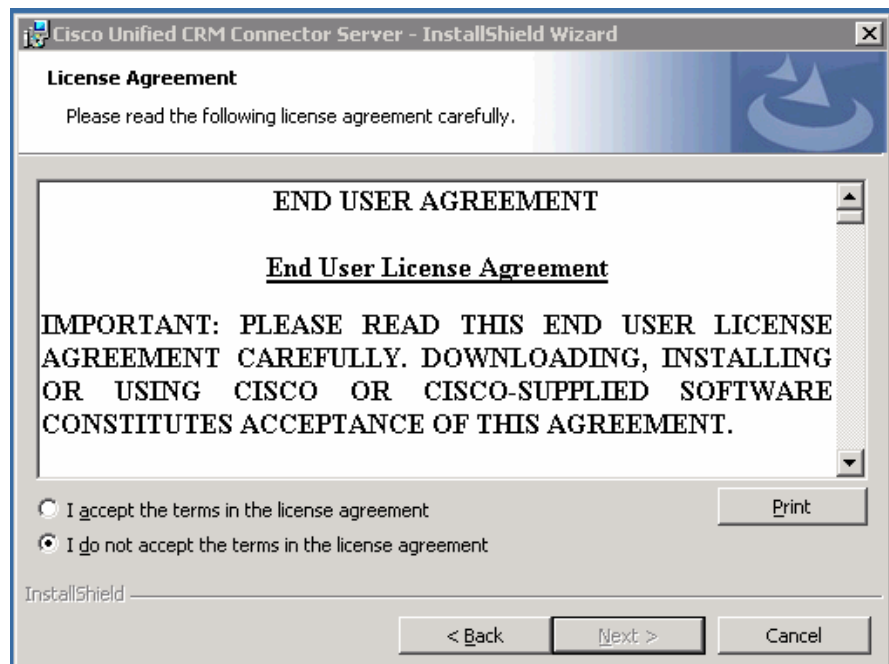
1. Select the Install CRM Connector Server Option from the selected component selection page:



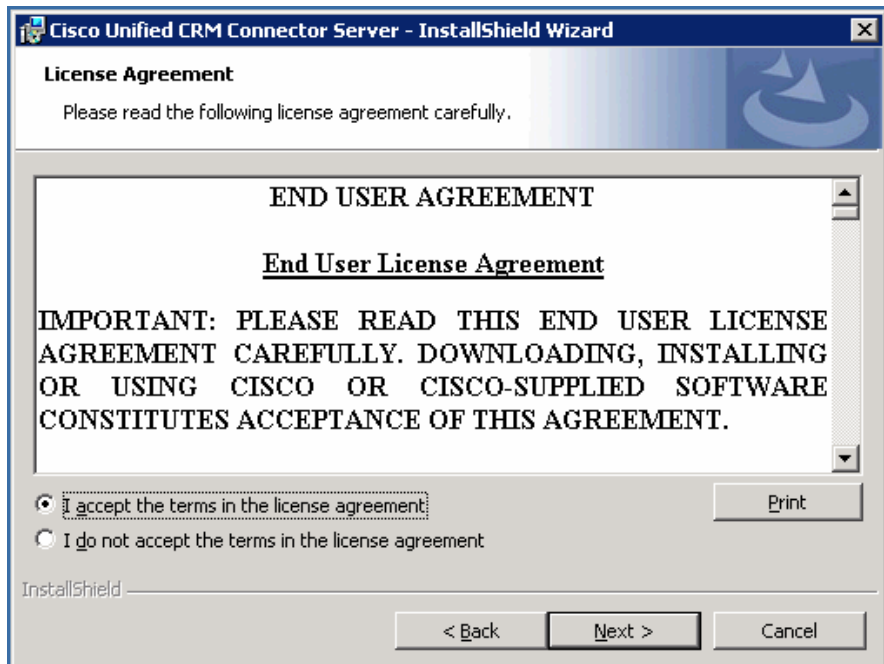
Step 2: Follow the Install Wizard and accept the end user license agreement.



- You are greeted with the InstallShield Wizard dialog for Cisco Unified CRM Connector Server: press Next to continue.
- You are prompted to accept the End User License Agreement (EULA)

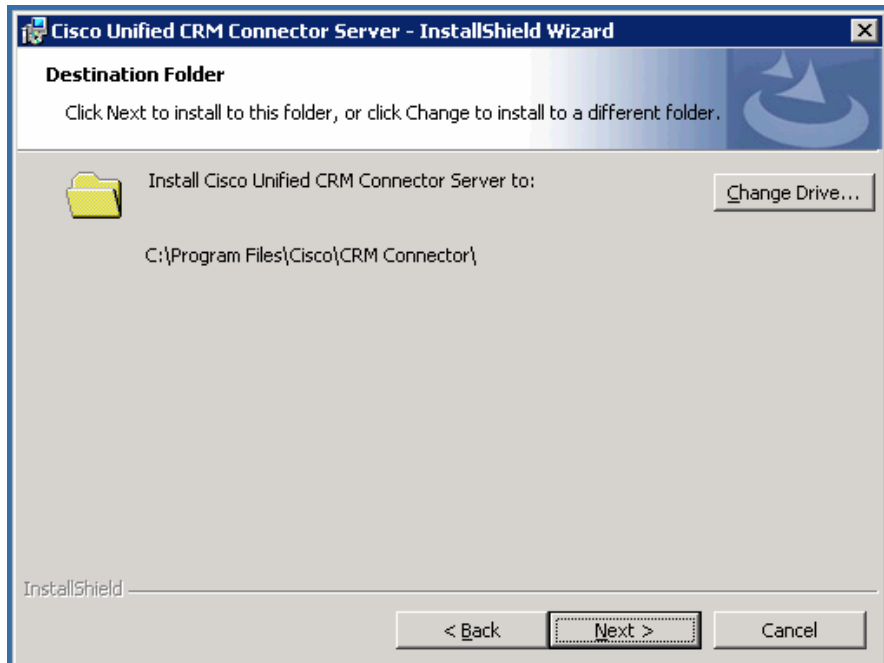


- Read and then accept the EULA by pressing the radio button labeled “I accept the terms in the license agreement.” Then press Next to continue.

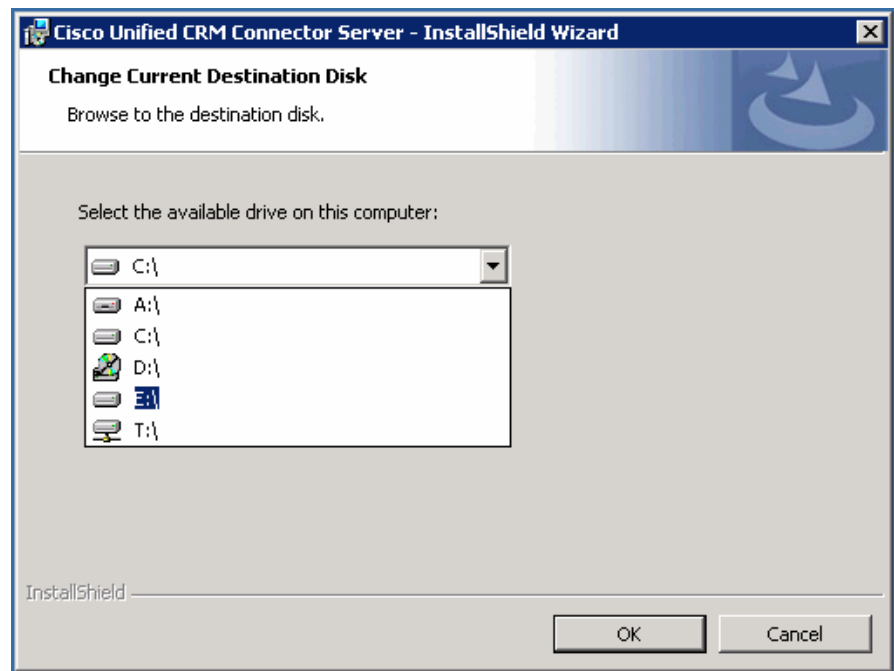


Step 3: Select the target installation drive.

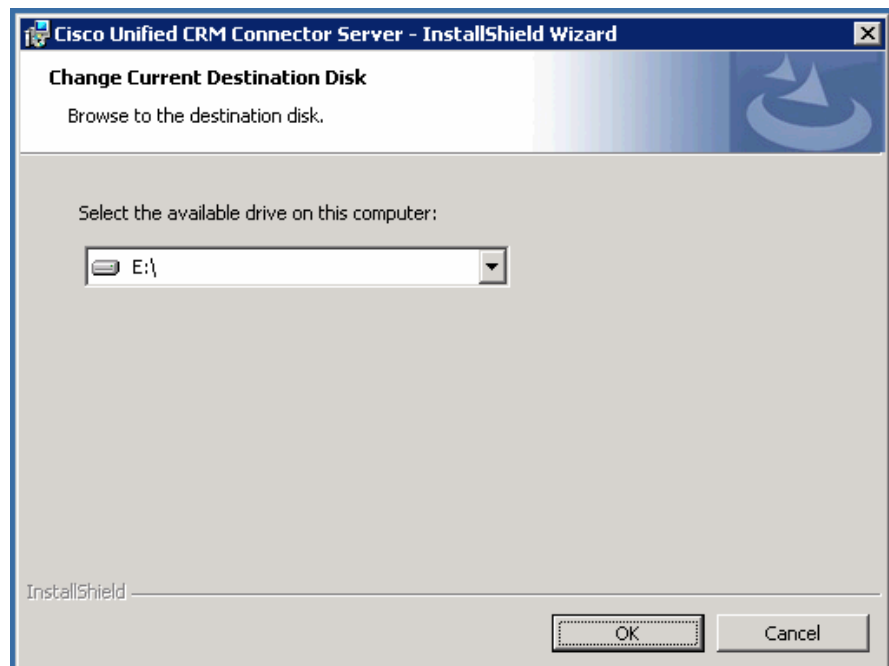
- You are next prompted to select a drive location. The installer defaults to install the C: drive. The directory path is fixed, but you may specify the target drive. If you wish to change the drive, press the “Change Drive” button.” Otherwise continue by pressing Next.



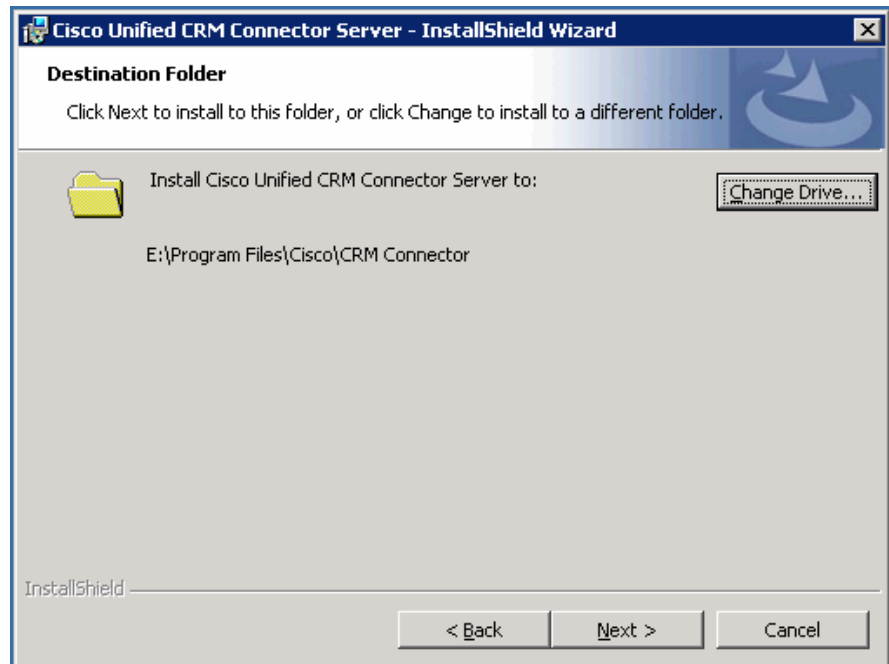
- If you choose to change the target drive you are prompted to select a new drive.



- After selecting the drive and pressing OK.

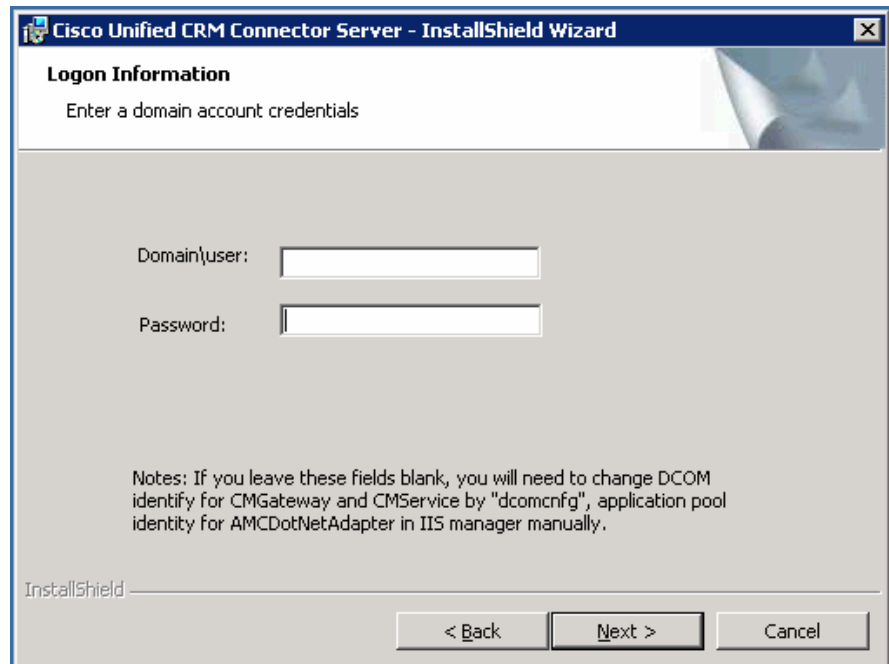


- You will return to the drive selection page; press Next to continue.



Step 4: Optional – Specify DCOM authentication credentials.

- Next you will be prompted for DCOM authentication credentials. Entering credentials here will automatically configure any DCOM settings; alternatively you may manually configure DCOM settings using the **dcomcnfg** utility as described below.



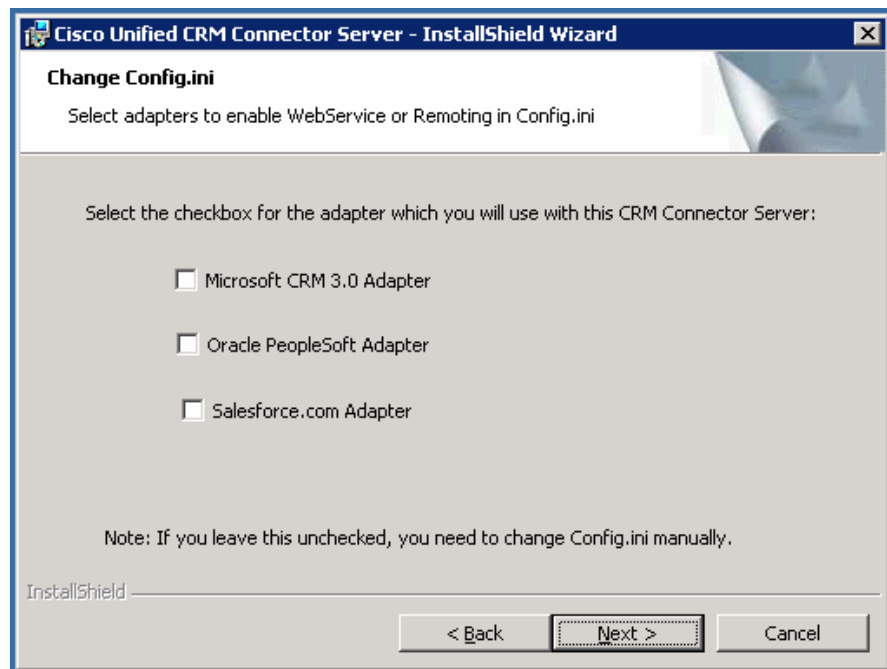
Note: DCOM requires fully qualified user credentials, which require machine or domain scoping. The user name must include either the domain or the machine name (if the user account is not a domain account). If you fail to enter fully qualified user credentials, you will be warned and prompted accordingly.

Note: If you do not enter user credentials, you may press Next and continue the install. However you must configure DCOM credentials manually, follow the instructions below in the **post install steps** section.

Warning: The DCOM user must have **local administration** privileges on the CRM Connector system. See below in the **post install steps** for user privilege configuration requirements.

Step 5: Select CRM application adapters.

- You are now prompted to select the CRM application adapter you are installing. Selecting an adapter will enable the CRM Connector config.ini file for the appropriate adapter. Otherwise you must manually enable the adapter.



Note: If you do not select an adapter, you must, enable it manually within config.ini.

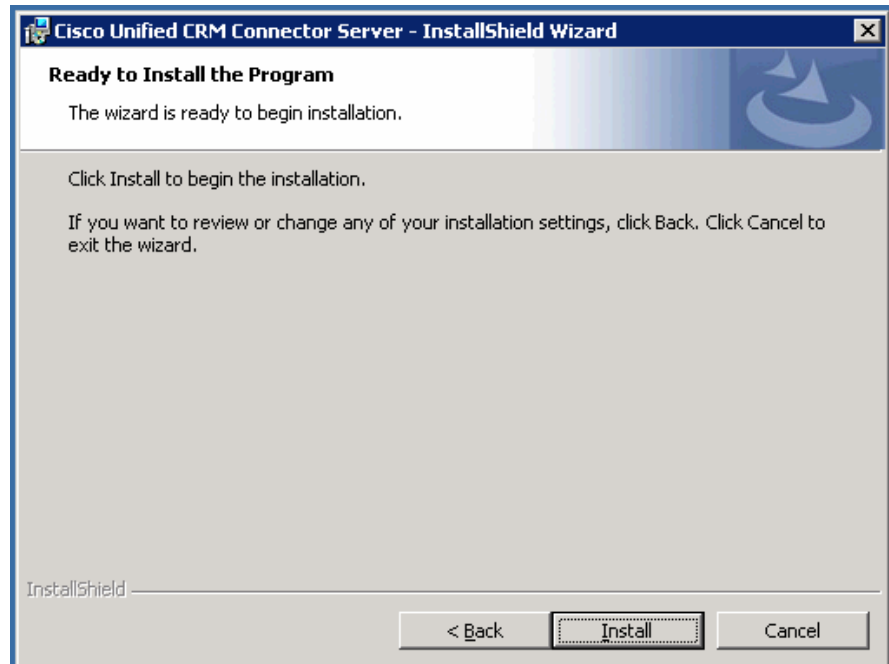
Note: You may choose more than one adapter type, if your system connects with multiple, different CRM applications.

Warning: This does not configure the adapter, configuration is a separate step.

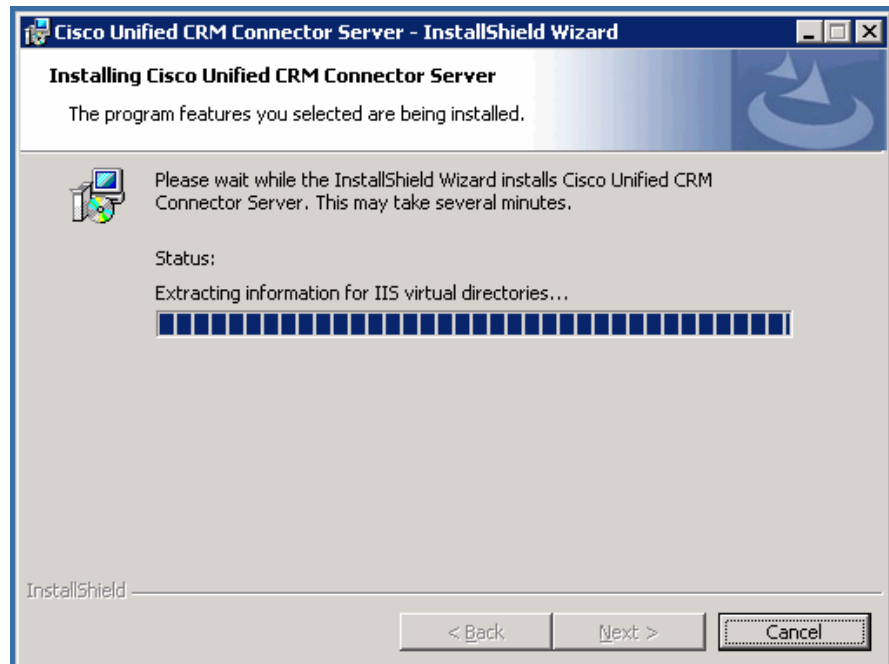
Warning: This does not install the adapter. Installation is a separate step.

Step 6: Install the software and finish the installation.

- You are now prompted to begin installing the software: press **Install** to start installing the software, **Back** to change installation options using this wizard, or **Cancel** to abort the installation.



- During the install a progress bar keeps you apprised of its status.



- Once the install is completed press Finish to complete the install and close the wizard.



What is Installed?

The installation program installs the CRM Connector Server services, the CRM Connector and the .NET Adapter components, which provide the

web services interface for the Administration Tool and for certain application adapters.

Table 3-1: CRM Connector Server Component Directory Structure lists the installed components and directories. The programs are installed in the directory tree under this parent directory:

<drive letter>:\Program Files\Cisco

where “drive letter” is the target install drive for the CRM Connector Server component.

Table 3-1: CRM Connector Server Component Directory Structure

| Sub-Directory | Component | Use | | | | | | | | | | | | | | |
|------------------------------------|------------------------------|---|---------------|------------------|--------------|---------------|---------------|-------------------|-----------------|--------------------|----------------|-------------------|--------------------|------------------------------|--------------|-----------------|
| ...\CRM Connector\MCIS\ | | Core services parent sub-directory. The configuration files, the core service executables and DLLs, and the log files are under this sub-directory. | | | | | | | | | | | | | | |
| | Config.ini | Configuration file. | | | | | | | | | | | | | | |
| ...\CRM Connector\MCIS\Server | | Core services application directory; log files directory is a sub-directory. | | | | | | | | | | | | | | |
| | AdminToolService.exe | This local service allows the Administration Tool web services to view and control the CRM Connector Server status. | | | | | | | | | | | | | | |
| | CMGateway.exe | The DCOM communications gateway service. This will be configured for DCOM in the post-installation steps. | | | | | | | | | | | | | | |
| | CMService.exe | The core services engine, this is the CRM Connector Server; it launches and manages all of the component service modules, the connector and the application adapter. | | | | | | | | | | | | | | |
| | Module DLLs | The rest of the files in this directory are DLLs that provide the module services listed in the CRM Connector Server architecture diagram. The configuration section of this chapter describes each components use and configuration. | | | | | | | | | | | | | | |
| | | <table><tr><td>Agent Manager</td><td>AgentManager.dll</td></tr><tr><td>Data Manager</td><td>DataStore.dll</td></tr><tr><td>Event Manager</td><td>Event Manager.dll</td></tr><tr><td>License Manager</td><td>LicenseManager.dll</td></tr><tr><td>Module Manager</td><td>ModuleManager.dll</td></tr><tr><td>Standard Interface</td><td>AMCMultiChannelInterface.dll</td></tr><tr><td>Work Manager</td><td>WorkManager.dll</td></tr></table> | Agent Manager | AgentManager.dll | Data Manager | DataStore.dll | Event Manager | Event Manager.dll | License Manager | LicenseManager.dll | Module Manager | ModuleManager.dll | Standard Interface | AMCMultiChannelInterface.dll | Work Manager | WorkManager.dll |
| Agent Manager | AgentManager.dll | | | | | | | | | | | | | | | |
| Data Manager | DataStore.dll | | | | | | | | | | | | | | | |
| Event Manager | Event Manager.dll | | | | | | | | | | | | | | | |
| License Manager | LicenseManager.dll | | | | | | | | | | | | | | | |
| Module Manager | ModuleManager.dll | | | | | | | | | | | | | | | |
| Standard Interface | AMCMultiChannelInterface.dll | | | | | | | | | | | | | | | |
| Work Manager | WorkManager.dll | | | | | | | | | | | | | | | |
| ...\CRM Connector\MCIS\Server\logs | | Default directory for all logs files. The log directory is set in the CRM Connector Server configuration. | | | | | | | | | | | | | | |

| Sub-Directory | Component | Use |
|--|------------------------|--|
| ...\CRM Connector\Dot Net Application Adapter\ | | This directory holds the .NET web services interface files. There are two sub-directories which are mapped as virtual directories in the IIS web server. Web services are implemented as ASP.NET generated web pages and exposed as .asmx files. See Chapter 6, Implementing the .NET Adapter for more information about the web services. |
| | SoapAdapter4DotNet.dll | This is the web services adapter, also referred to as the "Soap Adapter"; it provides interfaces to .NET web services for the Administration Tool and certain application adapters. |

Post Install Steps

Before you configure and test the CRM Connector Server there are some operating system configurations you must perform on the local server.

You must ensure that the CRM Connect Server user account has local system administration privileges. You must also adjust the local security policy as noted below.

If you did not specify DCOM authentication credentials as part of the install you must set those now as well. DCOM and service configuration steps are only required if you did not set user credentials during the CRM Connector Server install to assign a Windows user account.

Note: With DCOM enabled, this is a secure environment because DCOM components run locally and do not need to be configured for network access or launch.

The installation program installed two software services:

CMService – this is the primary service; it provides core services and runs all of the CRM Connector Server modules, the connector and the application adapters.

CMGateway – this provides DCOM communication for external service modules. .NET remoting and web services are used for application adapters.

Step 1: Configure your local user to run as a service

This step is required, even if you specified the user credential during your CRM Connector install. The user account with local administration rights will be used to launch the CMService and CMGateway services. This may either be a local or a domain account. This is done through the local security policy administration tool.

Because this account is used to manage services it is advisable to configure it so that the password never expires.

Note: This may violate the security rules for many organizations. You might address this by configuring this user so that it cannot login to interactive windows sessions; so that it only runs services.

Warning: If you configure the password with an expiration window, when the password expires the software will fail because the services cannot start.

1. Launch the Local Security Settings administration manager. From the Start menu select Administration Tools and then Local Security Policy.

Start → Administration Tools → Local Security Policy

2. This opens the “Local Security Settings” dialog. Use the navigation tree in the left pane to open the Local Policies tree and then select “User Rights Assignment.”

Security Settings → Local Policies → User Rights Assignment

3. This will list the named policies and their Security Settings in two columns in the right pane.
4. Assign the service user “Log on as batch job” privileges.
 - 4.1. From the right pane list of policies select *Log on as batch job*.
 - 4.2. Right click *Log on as batch job* and select Properties from the pop-up menu. This opens the Log on as batch job Properties dialog.
 - 4.3. Click the “Add User or Group button. This will present the Select Users, Computer or Groups dialog. Use this dialog to add the specific user or the local Administrator Group to this policy right. If this is a domain user, you will need to specify the domain location and the user.
 - 4.4. Press OK to add the user to the Policy list.
5. Assign the service user “Log on as service” rights.
 - 5.1. From the right pane list of policies select *Log on as service*.
 - 5.2. Right click *Log on as service* and select Properties from the pop-up menu. This opens the Log on as service Properties dialog.
 - 5.3. Click the “Add User or Group button. This will present the Select Users, Computer or Groups dialog. Use this dialog to add the specific user or the local Administrator Group to this policy right. If this is a domain user, you will need to specify the domain location and the user.
 - 5.4. Press OK to add the user to the Policy list.

Note: The next four steps (steps 2, 3, 4 and 5) are **OPTIONAL**. They configure DCOM default settings for the CMGateway and CMService services. *They are only necessary if you did not specify user credentials during the CRM Connector Server install.*

Step 2: OPTIONAL: Launch the Component Services dialog to configure DCOM configuration settings.

Use the DCOMCNFG configuration tool for these steps.

1. Use the Application Tools menu to launch the Configuration Services Manager from the Start Menu.

Select Start → Administration Tools → Component Services

Step 3: OPTIONAL: Set the default access permissions for this server.

1. Use the navigation tree on the left pane to open the Component Services tree; navigate to “My Computer”
Console Root → Component Services → Computers → My Computer.
2. Right click on *My Computer* in the left hand pane and select properties from the pop-up menu. This launches the *My Computer Properties* dialog.
3. Select the *COM Security* tab.
4. Select the *Edit Default* button under the Access Permissions group.
5. Use the *Add* button to add the Windows user account to the access permissions.
6. Check “Allow” for *Local Access*. Note that you do not need to set Remote Access rights; you may check ***Deny*** remote access rights to limit DCOM access from remote machines.
7. Press OK to apply the new security settings.

Step 4: OPTIONAL: Set DCOM Configuration for CMGateway.

You must configure security access, local endpoints and an “identity” for the CMGateway.

Security Access sets the DCOM authentication level strategy. This determines how and when a DCOM request is authenticated by the DCOM services. There are six security levels, each applying more stringent authentication. Security authentication takes time and resources that may impact overall system performance.

Because only users configured for DCOM access rights may launch and execute these functions, Cisco recommends setting the **Authentication Level to None**. Other Authentication Levels are discouraged and may affect system responsiveness.

Endpoints determine the network protocol used for DCOM communication. Only TCP/IP endpoints are supported.

Identity sets the user credentials that run the CMGateway service. You will use the user account with local administration privileges and the *logon as batch* and *logon as service* policy rights.

1. Use the left pane navigation tree to navigate to and select the DCOM Config sub-tree.
Component Services → Computers → My Computer → DCOM Config

2. This will list the DCOM components by name with their Application ID. The list is large; you will want to set the right pane view to *list*. From the “View” menu select list: **View → List** (the list option will receive a check mark).
You may also simply right click on the right pane and select **View→List** from the pop-up menu.
3. Find and right-click CMGateway from the list; select “Properties” from the pop-up menu. This launches the CMGateway Properties dialog.
4. Set the Authentication Level.
 - 4.1. Select the *General* tab.
 - 4.2. From the drop set the Authentication Level: **None**
5. Set the Endpoints.
 - 5.1. Select the *Endpoints* Tab.
 - 5.2. By default this shows *default system properties*. If “Connection-oriented TCP/IP” does not display, you will need to add it. If it is present you will need to set it as your default endpoint (Task 5.3)
Press *Add* to launch the **Select DCOM protocol and endpoint dialog**.
From the **Protocol Sequence** drop down select **Connection-oriented TCP IP**
Select **Use default endpoints** radio button and press OK.
 - 5.3. If Connection-oriented TCP/IP is already present, use the *Properties* button to launch the DCOM Endpoint Properties dialog. This modifies the endpoint details; select the *Use default endpoints* radio button to set this as the default endpoint.
6. Set the service run user account.
 - 6.1. Select the *Identity* tab.
 - 6.2. Select *This user* radio button.
 - 6.3. Enter the user account or use the *Browse* button to select a user account. Use the format: <domain name>\<user name>. Note: domain name may either be the local machine, for a local user account, or the domain name, for a domain account.
 - 6.4. Enter and confirm the password. The system checks user account and password and prompts you if the entry is not valid.

Step 5: OPTIONAL: Set DCOM Configuration for CMService.

Repeat the instructions for Step 4 selecting CMService.

Step 6: Configure web services in IIS.

After configuring DCOM services you will need to configure the .NET adapter services managed by IIS. As with the DCOM configuration, web services configurations assigns user credentials so that remote anonymous applications may execute web services functions in a secure configuration. The web services provide access to CRM Connector Server functions through a public interface published in the Administration Tool and used by some application adapters, such as the PeopleSoft.

You will use the Internet Information Services (IIS) Manager to configure the web services; you may also access this from the Computer Manager.

1. Launch IIS Manager:

Start → Administration Tools → Internet Information Services (IIS) Manager.

2. Use the left pane navigation tree to select Internet Information Services and select the installed computer. If running locally this will show as “(local computer)”, but you can run this from a remote machine.
3. Activate ASP.NET V2.0 web services extensions.
 - 3.1. Select Web Services Extensions from the left navigation pane.
 - 3.2. This shows configured web services extensions and their current permission status in the right pane: either Prohibited or Allowed.
 - 3.3. **Enable ASP.NET.** Check the status of ASP.NET v2.0.50727. If the status is prohibited you **must** enable it, continue with Task 3.4, otherwise you are done with this task and may continue with Task 4.
 - Select ASP.Net v2.0.50727 in the right view pane.
 - Press the **Allow** button to the left of the web services extensions list in the right hand pane.
4. Expand the Web Sites tree, this will list all of the Web Sites configured for this IIS service. The default configuration has one web site named “Default Web Site” this is where the Cisco web services components are installed.
5. Select *Default Web Site* in the navigation tree in the left pane. This will list the virtual directories installed on this web site in the right pane. You will be configuring these web services virtual directories:
 - AMCDoNetAdapterWebService
 - AMCDoNetEventAdapterWebService
6. Configure AMCDoNetAdapterWebService
 - 6.1. Right click the virtual directory in the right pane: AMCDoNetAdapterWebService and select *Properties* from the pop-up menu to launch AMCDoNetAddapterWebService properties dialog.

- 6.2. On the Virtual Directory tab verify the “Application Name” field is *AMCDotNetAdapterWebService* if the field is blank or if other information is present change it to this name.
- 6.3. In the “Application pool” drop down be sure that *AMCDotNetAdapter* is selected. If it is not, set it using the drop down.
- 6.4. Select the Directory Security Tab.
- 6.5. Click the *Edit* button in the Authentication and access control group at the top of the dialog. This launches the Authentication Methods dialog.
- 6.6. Select (check) *Enable anonymous access* at the top of the dialog.
- 6.7. Enter the user name and password for the CRM Connector Server account; when you press OK to leave this dialog you will be prompted to confirm the password in another pop up text box. If the passwords do not match you will need to re-enter them.

Warning: This does not check to be sure the user name and password are correct. If later you find that web services are not working, try re-entering the password.

Warning: If the user account password expires or changes for other reasons, web services will stop working; you will need to enter the new, changed password.

7. Configure the *AMCDotNetEventAdapterWebService* by repeating the instructions in task six (6) for this web service.
8. Configure the Application Pool access rights.
 - 8.1. Select *Application Pools* from the navigation tree in the left hand pane. This will list configured application pools, you will configure the *AMCDotNetAdapter* application pool.
 - 8.2. Select and right click *AMCDotNetAdapter* in the right pane. Select properties from the pop-up menu. This launches the *AMCDotNetAdapter Properties* dialog.
 - 8.3. Select the *Identity* tab in the properties dialog. This shows the Application pool identity dialog. The default configuration will show the *Preferred* radio button selected with the “Network Services” setting.
 - 8.4. Select the *Configurable* radio button and enter the user account and password information for the web services application pool. When you press OK you will be prompted with a pop up text box to confirm the password.

Warning: This does not check to be sure the user name and password are correct. If later you find that web services are not working, try re-entering the password.

Warning: If the user account password expires or changes for other reasons, web services will stop working; you will need to enter the new, changed password.

Step 7: Test the web services pages.

Test the web services by launching the web service ASP.NET asmx page under the web service virtual directory.

Note: You may only launch web services pages in an IE browser running on the local IIS machine. If you try to launch these remotely you will receive an error web page. You may launch these from within the Internet Information Services (IIS) Manager by right clicking on the asmx file in the web services virtual directory and selecting *Browse* from the pop up menu or you may enter the URL directly in the IE browser.

Example launch from the IIS Manager:

- From the navigation tree in the left pane select the AMCDotNetAdapterWebService.
- Right click TelephonyServices.asmx listed in the right hand pane and select Browse from the pop up menu. This will launch the WorkTopManagement web page which lists the following services links:

DeRegister
GetLoggedInInfo
GetWorkModes
LogIn
LogOut
Register
SetWorkModes

Note: These functions will not work until the CRM Connector Service is started, but you will be able to view the web services page.

Warning: If you receive a server error the IIS or web services may not be configured properly. Check to be sure that ASP.NET v2.0 is allowed and that you have configured the user names and passwords correctly in the virtual directories and the application pool.

This completes the post-installation steps. You may now configure the CRM Connector Server.

Configuring Core Modules for CRM Connector Server

This section describes how to configure the core modules. Once the core modules are configured, you may configure the Null Connector to validate the configuration and operation of the CTI Connector Server.

Configure core modules in the config.ini file.

Most CRM Connector Server components are configured using a **config.ini** file. This file is installed in the CRM Connector sub-directory under the parent directory tree (see Table 3-1: CRM Connector Server Component Directory Structure). This is a rather old, but extremely flexible and accessible Windows configuration technique.

You must edit this file to enter information specific to your server and your implementation. Use any text editor to edit the config.ini file.

You may rename the config.ini file or move it to another location. If you do this you must change the MCMS_INI environment variable to point to the fully qualified file name: that is the file name with the drive letter and full directory path.

Warning: If you move or rename the config.ini file some Administration Tool configuration features may not work, and you may need to edit the config.ini file manually.

Step 1: Verify the MCMS_INI environment variable setting and be sure that it matches the config.ini file location.

You can verify the MCMS_INI environment variable from within a command prompt using the set command.

1. Open a command prompt from the start menu or from a system desktop icon. **Start → run → cmd**
2. Enter the command *Set MCMS_INI*. This will display the MCMS_INI variable information. The default location is on the install drive in CRM Connector sub-directory.
3. Verify the file location (that it exists) by entering the fully qualified file name in a directory command.

At startup, the CRM Connector Server checks MCMS_INI environment variable for the location and name of the config.ini file. If the config.ini file is not found the service aborts with this error message:

The CMService on Local Computer started and then stopped. Some services stop automatically if they have no work to do, for example, the Performance Logs and Alerts service.

After this failure, no log files are created.

When the config.ini file is present, CRM Connector Server loads and parses it. It then launches the appropriate modules based on the configuration.

Config.ini sections

The config.ini file is divided into sections. There is one section for each configured module, one global section and a section for the Administration Tool configuration. Not all modules will be configured for your environment. Table 3-2: Config.ini Modules, Sections, DCOM Class and Log File Names lists the default modules, the config.ini section names and their use.

A section begins with a header with the section name in brackets. For example, the Global section header is: **[Global]**.

Key-Value Pairs

Each section contains configuration key-value pairs. These take the form **key=value**. There can be spaces in a key-value pair. Here are some sample key-value pairs:

TracePath=F:\ProgramFiles\Cisco\CRM Connector\MCIS\Server\Logs

ModuleClass=AgentManager,AgentManager.AMCAgentManagerModule

Most key-value pairs take only one parameter. Some, such as the ModuleClass key and the Module key take two parameters, comma delimited.

If there is a leading space the key-value pair is ignored. There may not be white space within a key-value pair: the key-value pair ends after the first space or a carriage return.

Comments

You may comment your config.ini file. Any leading space or non-key value character is treated as a comment. However, traditionally the hash key (also referred to as the “pound” or “octothorp”) “#” is used to mark a commented out line.

Here is an example commented out key-value pair, its configuration is not applied: **# TraceLevel=2.**

White space, including blank lines, is ignored and may be used to make the configuration file more readable. Use the hash to indicate comments. Lines with leading spaces are ignored and should be avoided as they may introduce errors.

Table 3-2: Config.ini Modules, Sections, DCOM Class and Log File Names

| Section Name | Module Class Name / Log File name | Module DCOM Class Name | Use |
|-------------------|--|---|--|
| [Global] | No module / No log file | None | The global section sets default key values for log locations and trace levels. These values may be over-ridden in each module section. |
| [ModuleManager] | No class name/ ModuleManager.log | None (internal to CRM Connector)Server) | This manages the operation of all other modules. It starts, stops, and monitors every module configured. Configure modules in the module manager section. This section maps the module names to module class. It also maps the module class to the DCOM class name; to enable module manager to launch the module DCOM process. |
| [AgentManager] | AgentManagerClass / AgentManager.log | AgentManager.AMCAgentManager-Module ** | This handles agent state such a work state, and queue login status. |
| [Data Store] | DataStoreClass / DataStore.log | DataStore.AMCMemoryDataStore | This manages call information also known as call-associated data. |
| [DataStoreServer] | ServerDataStoreClass / DataStoreServer.log | DataStore.AMCRemotingDataStore.-DataStoreServerModule | This is used for shard data stores; it manages data coordination and communication with a Data Store client that runs on CRM Connector Servers that use this remote data store. |
| | DataStoreServerClass / AA_ServerDataStore.log | DataStore.AMCMemoryDataStore | This is the shared data store component on the server for a shared Data Store. |
| [DataStoreClient] | DataStoreClientClass / DataStoreClient.log | DataStore.AMCRemotingDataStore.-DataStoreClientModule | This is used for shared Data Store; it manages the data coordination and communication with a Data Store Server. |
| [EventManager] | EventManagerClass / | AMCEventManagerModule.AMCEvent-ManagerModule** | This manages internal events, synchronous and asynchronous events between modules. |

| | | | |
|-----------------------|---|---|--|
| | | | |
| [LicenseManager] | LicenseManagerClass / LicenseManager.log | LicenseManager.AMCLicenseManager- Module | This is responsible for managing configured licenses and monitoring license use. |
| [WorkManager] | WorkManagerClass / WorkManager.log | WorkManager.AMCWorkManager | Manages local server queues. |
| StandardizedInterface | StandardizedClass / StandardizedInterface.log | AMCMultiChannelInterface.AMC- Application** | This maintains the multi-channel interface state for application integration. |
| [CMGateway] | CMGatewayClass / CMGateway.log | CMGateway.CMGatewayModule | This out-of-process module runs as a configured service. It provides distributed DCOM connections. |
| [SoapAdapter] | SoapAdapter4DotNet_- ProgID / SoapAdapter.log | SoapDapter4DotNet.SoopAdapter- Module** | .NET Adapter to support Administration Tool and application adapters such as the PeopleSoft adapter. |
| [RemotingEndpoint] | RemotingEndpointClass / RemotingEndPoint.log | AMCDotNetAdapterRemotingLibrary.- RemotingModule** | .NET remoting creates .NET remoting endpoints for direct communications. This bypasses .NET web services for a faster, more direct communication. It is used by application adapters such as the Salesforce.com adapter. |
| [CTIModule]* | CicsoCTI / CTIModule Log | Cisco.AMC_Cisco | Cisco connector for UICM, UCCE, and UCCX |
| | CTINullClass / CTIModule.log | CIT_NULL.AMC_CTI_NULL | Null CTI connector used for testing configurations. |
| [AdministrationTool] | None/ AdministrationTool.log | None | This configures the administration tool. The administration tool runs as a service on a CRM Connector Server and uses the config.ini file. |

*You may use different names to run multiple CTI sites on one CRM Connector Server.

** There is no hyphen in the actual class name. Hyphens in DCOM class names are "softphones" used to split the class name so that it fits on a single line.

Global Section

The global section holds global configuration key-value pairs that apply as a default for all modules. Table 3-3: Global Configuration Keys lists the global section configuration keys, their use and their valid values.

Any module may include these keys to override the default values set in the global section.

Table 3-3: Global Configuration Keys

| Key | Valid Values – Meaning | Meaning / Use |
|--------------|---|--|
| TraceEnabled | 0 – Trace disabled 1 – Trace enabled | Enables or disables log tracing. The default value is 1 == on. |
| TraceLevel | 1 – Errors Only 2 – Errors and Warnings 3 – Errors, Warnings and Information 4 – Errors, Warnings, Information and Debug (diagnostics) Default: 4 Note: some modules support higher debug levels with trace values greater than 4. | Sets the trace log level. Within the log file each log entry line has a prefix letter: E – Errors W – Warnings I – Information D – Debug / diagnostic |

| Key | Valid Values – Meaning | Meaning / Use |
|----------------|--|--|
| TraceFile | A valid Win32 Filename. Default: the module section name with “.log” suffix. | Set the log file name. Note that most modules override this value and it is often not commented out in the global section. |
| TracePath | Valid Win32 file path, fully qualified. Default: <install drive letter>:\Cisco\CRM Connector\MCIS\Server\logs | Log file directory location. |
| TraceMaxSize | Positive integer value. Default: 1024 (1 MB) | The maximum trace file size in KB. Tracing wraps to top of file when max size is reached. |
| MessageLibrary | DLL name with message resources. | Holds messages as Windows resources. |
| EventManager | EventManager | The default event manager for all modules. |

Example 3-1: Global Config.ini Section

```
###
# Global Keys
###
[Global]
TraceEnable=1
TraceLevel=4
TracePath=c:\ProgramFiles\Cisco\CRM Connector\MCIS\Server\Logs
TraceMaxSize=2048
# MessageLibrary=AMCMessages.dll
# EventManager=EventManager
```

Module Manager Section

The module manager configures the modules for the CRM Connector Server.

The module manager has two types of keys. The first define module types as a ModuleClass and the second defines module instances as a Module.

There are two entries for each configured module within the Module Manager, one to define ModuleClass and another to define a module instance. A module class may be defined but not used – has no module entry. It is an error to configure a module instance if its ModuleClass has not been defined.

For clarity, the sample [ModuleManager] section below separates the CTI channel configuration and the remoting endpoint from other, more fundamental module class and module definitions. These represent the connector module and the adapter connection for most adapters.

Most application adapters are not configured within the config.ini file. They rely on the .NET Adapter for remoting or web services (Soap), and run outside the CRM Connector Server, on application server machines or agent desktops.

Table 3-4: Module Manager Keys

| Key | Valid Values – Meaning | Meaning / Use |
|-------------|---|---|
| ModuleClass | Format: ModuleClass= <ClassName>,<ProgID> Numerous values (see Table 3-2: Config.ini Modules, Sections, DCOM Class and Log File Names) | Defines a module type and associates the DCOM program ID name. DCOM uses this to lookup the UUID and launch the module. |
| Module | Format: Module= <ModuleName>,<ClassName> Numerous values (see Table 3-2: Config.ini Modules, Sections, DCOM Class and Log File Names) | Defines an instance of a module. The module is configured in the [<ModuleName>] section within the config.ini. file. |

Example 3-2: Module Manager config.ini Section

```
## Define Module Classes
ModuleClass=AgentManagerClass,AgentManager.AMCAgentManagerModule
ModuleClass=DataStoreClass,DataStore.AMCMemoryDataStore
ModuleClass=EventManagerClass,AMCEventManagerModule.AMCEEventManagerModule
ModuleClass=LicenseManagerClass,LicenseManager.AMCLicenseManagerModule
ModuleClass=WorkManagerClass,WorkManager.AMCWorkManager
ModuleClass=StandardizedClass,AMCMultiChannelInterface.AMCApplication
ModuleClass=CMGatewayClass,CMGateway.CMGatewayModule
ModuleClass=SoapAdapter4DotNet_ProgrID,SoapAdapter4DotNet.SoopAdapterModule

### Define Module instances
Module=AgentManager,AgentManager
Module=DataStore,DataStoreClass
Module=EventManager,EventManagerClass
Module=LicenseManager,LicenseManagerClass
Module=WorkManager,WorkManagerClass,
Module=StandardizedInterface,StandardizedClass
Module=CMGateway,CMGatewayClass
Module=SaopAdapter,SoapAdapter4DotNet_ProgrID

### CTI Channels
# NULL Connector -- ModuleClass=CTINullClass,CTI_NULL.AMC_CTI_NULL
# NULL Connector -- Module=CTIMoudle,CTINullClass
ModuleClass=CiscoCTI,Cisco.AMC_Cisco
Module=CTIModule,CiscoCTI

### Remoting EndPoint
ModuleClass=RemotingEndpointClass,AMCDotNetAdapterRemotingLibreary.RemotingModule
Module=RemotingEndpoint,RemotingEndPointClass
```

Agent Manager Section

The agent manager module maintains the agent work state. This includes the agent's login state with the ACD and the current work mode. There are two configuration keys.

Table 3-5: Agent Manager Keys

| Key | Valid Values | Meaning / Use |
|--------------------------------------|---------------|---|
| SuppressPendingWorkModeChange | True False | Defines whether to raise a work mode changed event but the connector reports “active work,” case sensitive. |
| RaiseNewWorkEventForUnknown-WorkTops | True False | Change this setting only if directed by Cisco TAC support. |

Work Manager Section

The work manager section has no configuration keys.

Data Store Section

The Data Store maintains contact associated data. This includes standard call information such as ANI and DNIS, customer entered digits, IVR data and bookmarks, and other information used to transfer agent work context from the CRM business application with calls.

This makes the Data Store a critical component, with a central role in the major contact center functions: presenting the screen pop and coordinating call information and context between the voice channel and the business application.

Because of this central role and the need to coordinate information across multi-channel, multi-instance deployments, there are two configurations for the Data Store: the stand-alone Data Store and the shared Data Store.

The stand-alone Data Store is used in single instance deployments of the CRM Connector Server; where all the services and information can be managed in a single instance. This Data Store is configured as an in-process module for the CRM Connector Server service CMService.

The shared Data Store has remoting features that allow it to hold data for and communicate with one, two or more CRM Connector Servers. It is implemented for either of two reasons:

- In order to scale a single-instance for large centers. The Data Store keeps call information in memory, which may reduce performance with large volumes of calls, high rates of transfers, or applications that transfer large amounts of information. By remoting the Data Store, it can reside on its own CRM Connector Server instance, with the connector and adapter running on their own instance.
- For transferring calls with context in centers with multiple CRM Connector Servers supporting multiple sites or multiple instances. The shared Data Store may reside on a single CRM Connector Server instance or it may reside on its own CRM Connector Server instance

You may configure more than one shared data store for an enterprise contact center. Each shared data store establishes a group of users, application adapters and channel connectors that can share call data and transfer calls with data context.

Stand-alone Data Store Configuration.

The stand-alone Data Store is configured as a single module of the CRM Connector Server. It consists of one class and one instance of Data Store. Its parameters maintain the integrity of the managed information, setting clean up intervals and the data expiration timeout. These management times are needed to ensure that data is properly associated with the phone call in environments where call IDs can repeat in a short timeframe.

It follows the standard module configuration:

Step 1: Define the Data Store module class.

In the Module Manager section, enter the module class and instance:

ModuleClass=DataStoreClass,AMCMemoryDataStore

Module=DataStore,DataStoreClass.

Step 2: Define the Data Store section and set the DataStore parameters:

The section name is “DataStore,” the optional parameters, their meaning and default values are shown in Table 3-6: Stand-Alone Data Store Parameters

Table 3-6: Stand-Alone Data Store Parameters

| Key | Valid Values – Meaning | Meaning / Use |
|-----------------|-------------------------------|--|
| CleanupInterval | Positive integer (in minutes) | Intervals in minutes between data clean up. If zero (0), then no clean up is performed. Default is 10 minutes. |
| DataExpiration | Positive integer (in minutes) | Maximum duration to hold a data index before it is subject to clean up. Default is 60 minutes. |

Shared Data Store Configuration.

There are two separate configurations for the shared Data Store:

- the data store server hosts the data store and its information;
- the data store client connects with and uses the server data store.

The data store server may be a dedicated data store, in which case there is no data store client on the data store server system, or it may be co-reside with connector and adapter instances.

The data store client must be configured on all remote CRM Connector Servers that use the shared data store and on the data store server if it co-resides with a connector.

Step 1: Configure the Data Store Server.

The Data Store server has a data store, the data store server and a data store client.

1. Define the data store module class and instance in the Module Manager. This uses the same data store class but uses a slightly different data store instance name:

ModuleClass=DataStoreClass,AMCMemoryDataStore

Module=AA_ServerDataStore,DataStoreClass

2. Define the Data Store server for remoting. This uses a different class Data Store class, the DataStoreServerClass.

ModuleClass=DataStoreServerClass,AMCRemotingDataStore.DataStoreServerModule

Module=DataStoreServer,DataStoreServerClass

3. Configure the Data Store server section. This requires a remoting port and also takes the data store configuration parameters.

NOTE: The standard data store remoting port is 5666, however you may use a different port addresses. If a .NET remoting adapter or other .NET remoting component also resides on this CRM Connector Server instance, you must **use the same port address** for the server data store remoting port and the .NET remoting adapter port.

Table 3-7: Server Data Store Parameters

| Key | Valid Values – Meaning | Meaning / Use |
|-----------------|--|--|
| RemotingPort | Any valid port address If .NET remoting is also implemented on this CRM Connector Server instance, you must use the same port address for both. Default: N/A | This is the remoting port address. This uses.NET remoting for communication between the Data Store server and its clients. The must be configured, it does not have a “default” value. The standard value is 5666. |
| CleanupInterval | Positive integer (in minutes). Default: 10 minutes | Intervals in minutes between data clean up. If zero (0), then no clean up is performed. |
| DataExpiration | Positive integer (in minutes). Default: 60 minutes | Maximum duration to hold a data index before it is subject to clean up. |

Step 2: Configure the Data Store Client.

The Data Store client connects to and communicates with the data store client through the remoting port. The data store client must be defined on the data store server and on all data store clients.

1. Define the data store module class and instance for the data store client:
ModuleClass=DataStoreClientClass,AMCRemotingDataStore.DataStoreClientModule
Module=DataStore,DataStoreClientClass
2. Configure the data store client parameters in the as the [DataStore] section; assign the host data store server name and its port. (See Table 3-8: Data Store Client Parameters.)

Note: To configure the data store client on the data store server instance specify “Local Host” as the DataStoreServerHost name. For a remote client, specify the IP address of DNS name of the host machine.

Table 3-8: Data Store Client Parameters

| Key | Valid Values – Meaning | Meaning / Use |
|---------------------|---|---|
| DataStoreServerHost | The host name, IP address or DNS name of the server machine. On the server machine you may specify “LocalHost” Default: N/A | Used to connect with the Data Store server machine. |
| DataStoreServerPort | This must match the data store server remoting port. Default: None (Standard is 5666) | The host server data port address. This must be configured. It does not have a “default” value. The standard value is 5666. |

Event Manager Section

The event manager manages synchronous and asynchronous events between modules.

Table 3-9: Event Manager Keys

| Key | Valid Values – Meaning | Meaning / Use |
|-------------------|--|--|
| ThreadPoolSize | Range is 1 to 64 Default: 5 | Sets the thread pool for servicing events. Notes: For optimal throughput the threadpool should equal the number of server processors. For optimal response, it should equal the number of agents; if there are more than 64 agents set this to 64. |
| IoPortReadTimeout | Range is 3000 to 50000 Default: 3000 | I/O port timeout in seconds. |
| UseSafeMode | Yes – use safe mode No – do not user safe mode. Default: Yes (case sensitive) | Spin (launch) a new thread and timeout every event raised. |
| RaiseTimeout | Range is 20 to 100 Default: 20 | The delay before timing out an event raise when UseSafeMode = Yes. |

Standardized Interface Section

The standardized interface maintains multi-channel application state. It must be configured to associate with an Agent Manager and may be configured to return error codes.

Table 3-10: Standardized Interface Keys

| Key | Valid Values – Meaning | Meaning / Use |
|------------------|---|--|
| AgentManager | Name of agent manager module. Default: AgentManager | Identifies agent manager associated with standardized interface. |
| ReturnErrorCodes | True False Default: False | Returns error codes |

CMGateway Section

The CMGateway provides distributed connections to the CRM Connector Server through DCOM. There is one configuration key, The InstanceName.

Table 3-11: CMGateway Interface Keys

| Key | Valid Values – Meaning | Meaning / Use |
|--------------|---------------------------------------|---------------|
| InstanceName | A text string. Default: N/A | Service name. |

Remoting Endpoint Section

See Chapter 6: *Implementing the .NET Adapter*, the .Net Remoting configuration section.

Soap Module Section

See Chapter 6: *Implementing the .NET Adapter*, the .Net Soap Adapter configuration section.

License Manager Section

The license manager section manages license allocations and monitors license consumption. When all licenses are consumed the License Manager blocks additional users who would require a license.

The CRM Connector Server is assigned a license key that allocates a pool of licenses. Each agent user consumes a license through the connector as they log into the ACD. In addition, each connector and each application adapter consume a license. The license is consumed when the first agent uses the connector or the adapter.

Therefore use the following formula to determine the appropriate number of licenses in your license pool:

Number of agent users + number of connectors + number of adapters.

Note: the .NET Adapter consumes a single license.

Each licensed module is assigned a license key in the License Manager section. The license value is a 30 character alpha string. Your Cisco partner will provide and assist you with licensing your CRM Connector components.

Table 3-12: License Manager Keys

| Key | Valid Values – Meaning | Meaning / Use |
|------|---|---|
| MCIS | 30 character alpha string license generated through the license process. Default: n/a | CRM Connector Server license. Generated license for the core services; these licenses are allocated when the server starts and are consumed by agent users, connectors and adapters. |

| Key | Valid Values – Meaning | Meaning / Use |
|-----------|---|--|
| CTI_Cisco | 30 character alpha string license generated through the license process. Default: N/A | The Cisco UICM, UCCE, and UCCX connector license key. One license is consumed for each agent logged in and one is consumed by the operating connector. |
| AA-DotNet | 30 character alpha string license generated through the license process. Default: N/A | This is used and required for all application adapters; it licenses .NET communication for remoting and web services. |

Configuring the Null CTI Connector for Testing.

The Null CTI connector is a core module that can simulate phone calls and the responses of a CTI server. The Null CTI connector is configured in the CTIModule section. It does not need to be licensed.

Enable the Null CTI module by defining an instance of the CTINullClass. The CTI NullClass is defined with the CTI_NULL.AMC_CTI_NULL program ID.

Table 3-13: Null CTI Connector Keys shows the configuration keys and values for the Null C TI Connector.

Table 3-13: Null CTI Connector Keys

| Key | Valid Values – Meaning | Meaning / Use |
|----------------|--|---|
| Channel | Four (4) character string Default: CTI1 | The Channel ID. This identifies the channel and is used to associate agent requests with a specific CTI channel. The CTI channel name will show up in the log files on channel events and application commands. |
| InternalExtLen | Positive integer, less than or equal to the length of a dial sting. Default: 5 | The length of an internal extension. This is used to block screen pops on internal agent-to-agent calls. Most call centers use a dial plan that uses an internal station directory number that is less than the national PSTN dial string. Note: This will not block context screen pops on internal transfers or conferences, but may be used to delay the screen pop until the transfer (or conference) complete |
| DataStore | String, DataStore module name. Default: DataStore | This associates the data store with the CTI module; it is possible to configure multiple CTI modules on a single server as well as multiple data store instances. |

| Key | Valid Values – Meaning | Meaning / Use |
|----------------|--|--|
| ServerName | String Default: N/A | The name of the simulator server. Most CTI connections have an internal name and this simulate that name. |
| Simulator | Yes No Default: Yes | Enables the null telephony server to simulate a telephony channels. The default value is Yes. |
| SimulatedLines | Positive integer 1 to 5 Default: 2 | Number of lines per extension that should be simulated by the Null CTI connector. |
| KnownQueues | String Default: N/A | Defines a list of simulated queues that are considered “known” and therefore valid in the simulated CTI environment. For this simulator any queue values are acceptable; these are usually 2 or 4 digit numbers but may be any length. |

Example 3-3: Null CTI Connector Settings

```

###
# CTIModule
###
[CTIModule]
Channel=SIM1
ServerName=NULL
Simulator=Yes
SimulatedLines=2
InternalExtLen=4
KnownQueues=10,9100,2001,2002

```

4. IMPLEMENTING THE ADMINISTRATION TOOL

Purpose

This chapter describes how to install and configure the CRM Connector Administration Tool.

The Administration Tool is a browser based application that uses .NET web services to control, configure and monitor CRM Connector Servers. It can support more than one CRM Connector Server enabling management of all CRM Connector Servers in a multi-system enterprise.

This chapter covers:

- Administration Tool Features and Functions
- Planning for and Deploying the Administration Tool
- Installation Pre-Requisites
- Installing the Administration Tool
- Configuring the Administration Tool
- Configuring CRM Connector Server for the Administration Tool
- Testing the Administration Tool Implementation.

Before you begin

The Cisco CRM Connector Administration Tool is a web service that runs under Microsoft Internet Information Services (IIS). Install the Administration Tool on a system running IIS with .NET Framework V2.0 runtime installed. The IIS server must also be installed on all the CRM Connector Server machines managed by the Administration Tool.

Because the Administration Tool web services must access remote systems, it requires a Microsoft Domain user account to access remote services. This is an exception to the general requirement that Microsoft domain accounts are not required for accessing and using CRM Connector components.

You must also have either a production instance of Microsoft SQL Server or a local copy of Microsoft SQL Server 2005 Express installed for the Administration Tool's configuration data store. You may download MS SQL Server 2005 Express from the Microsoft download center. More recent versions should work, but you should test them or, better, check the release notes or with Cisco TAC.

Overview: Administration Tool Features and Functions

The Cisco CRM Connector Server Administration Tool provides a single management and monitoring point for the Cisco CRM Connector and its

components. It supports the needs of system administrators, agent supervisors and technical support personnel.

Key features of the Administration Tool:

- Browser-based central access to all CRM Connector Servers. The Administration Tool can remotely access configuration and log files and set configurations on multiple CRM Connector Servers throughout the enterprise.
- Individual user accounts with security access restrictions. The Administration Tool can be configured to support a variety of contact center roles. Super users have full access for CRM Connector Server administration. Lesser users can be restricted to viewing real-time server status or accessing and reviewing log files. Each user account is password protected.
- Review and modify CRM Connector Server configuration files [config.ini] remotely.
- Dynamic changes to global or individual module trace levels, without restarting the CRM Connector Server
- Update and apply license changes permanently and dynamically.
- View current log trace files remotely.
- View active agents (logged into the system) and their current work state.

Overview: Planning and Deploying the Administration Tool

The Administration Tool requires an existing CRM Connector Server implementation. It connects with the CRM Connector Server but may be installed on a separate machine, one dedicated to running web services. It connects with a communication service that runs on the CRM Connector Server and is configured on the CRM Communication. You should deploy one copy of the Administration tool to support all CRM Connector Servers in your environment.

There are no client configuration or deployment requirements because the tool is accessed through a web browser. Use Microsoft Internet Explorer to access the Administration Tool: it has been certified for access with the Internet Explorer 6.0 or higher.

Installation Pre-Requisites

The CRM Connector Server Administration Tool should be installed on a dedicated IIS server, although for small sites it may co-reside with a CRM Connector Server. It requires all of the supporting software as the base CRM Connector Server install:

- Microsoft Windows 2003 Server SP1 or SP2
- Microsoft Internet Information Services
- Microsoft .NET Framework Version 2.0
- ASP.NET enabled on IIS

In addition to these required operating environments, the Administration Tool also requires a Microsoft SQL Server instance. This may be either a production MS SQL Server or Microsoft SQL Server 2005 Express.

The instructions for installing and configuring these components are in Chapter 3: Implementing the CRM Connector Server.

Use the same Windows user account privileges, one with local administrations rights on the server you are installing Cisco Administration Tool onto.

Installing the Administration Tool

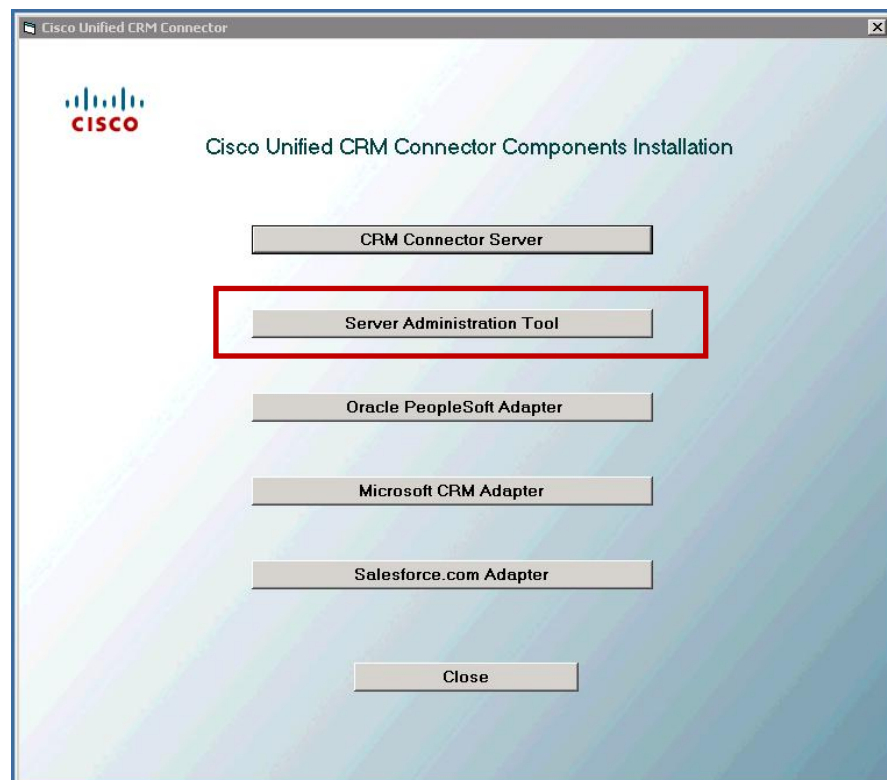
The CRM Connector Administration Tool software installation is straightforward; however you will need to perform a number of special post-install configuration steps.

There are only a few installation options. The install wizard prompts for the drive to install the Administration Tool upon and whether the database schema needs to be installed on the SQL Server (or SQL Server Express). shows the default directory structure and installed files.

If Microsoft .Net Framework V2.0 is not installed on the server InstallShield wizard will install it.

Step 1: Start the installation and select the Administration Tool Component.

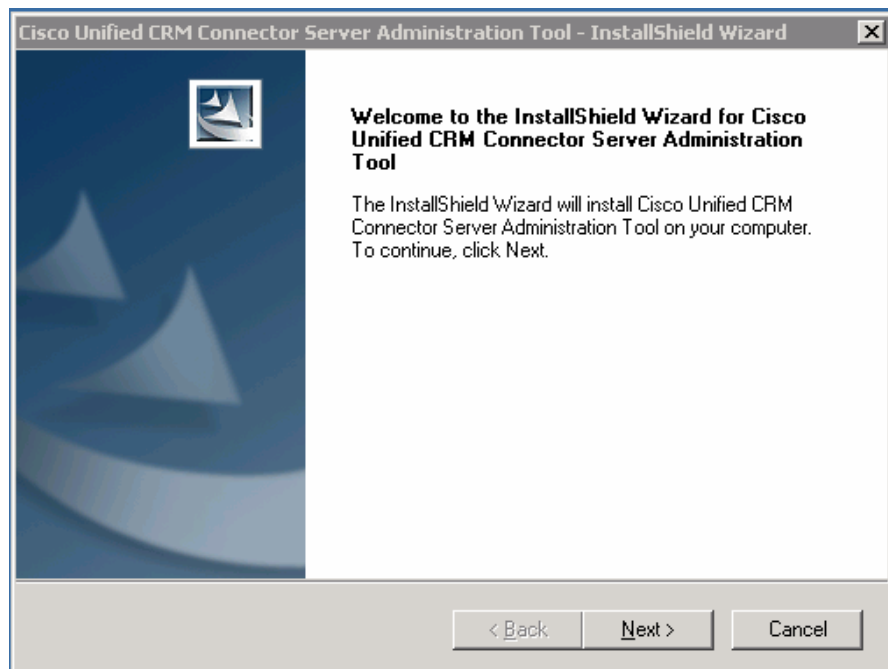
1. Select the Install Server Administration Tool Option from the component selection page:



Step 2: Start the Install Wizard, accept the EULA.



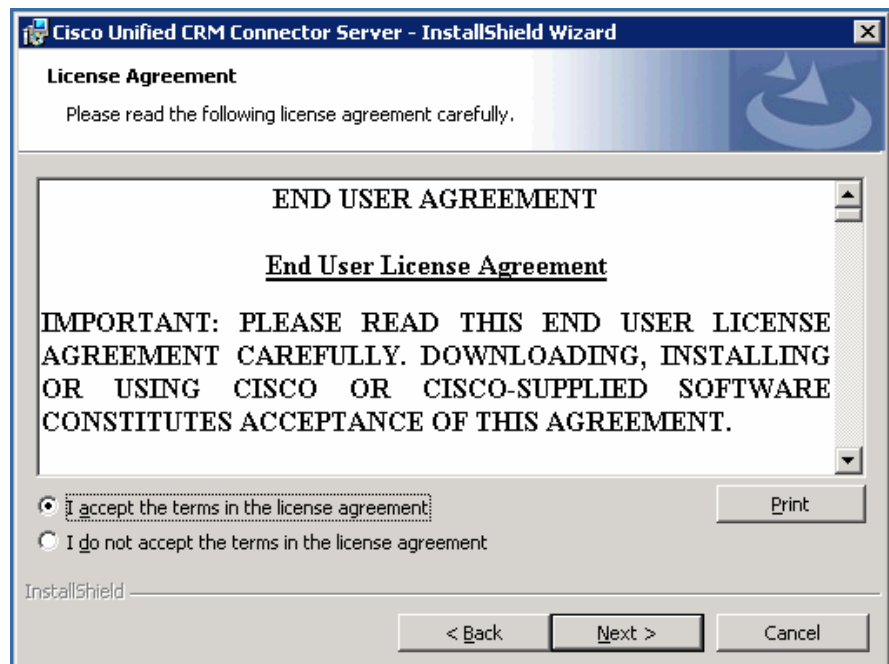
- You are greeted with the CRM Connector Server Administration Tool splash screen; this will display while the install prepares, then you are prompted with the initial InstallShield Wizard dialog.



- Press Next at the InstallShield Wizard welcome dialog to begin the install. (Pressing Cancel aborts installation.) You are prompted to accept the End User License Agreement (EULA)

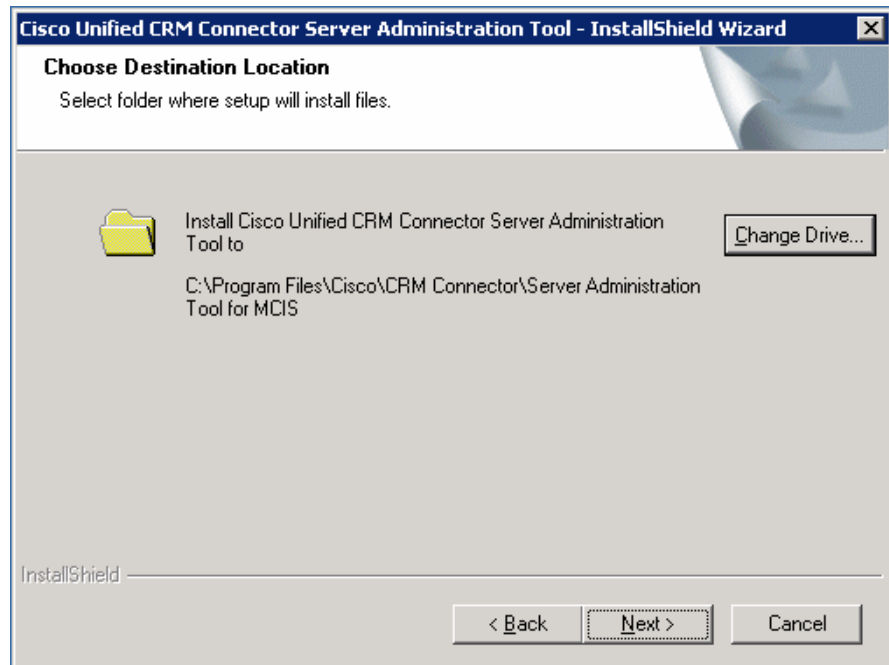


- Read and then accept the End User License Agreement (EULA) by pressing the radio button labeled “I accept the terms in the license agreement.” Then press Next to continue.

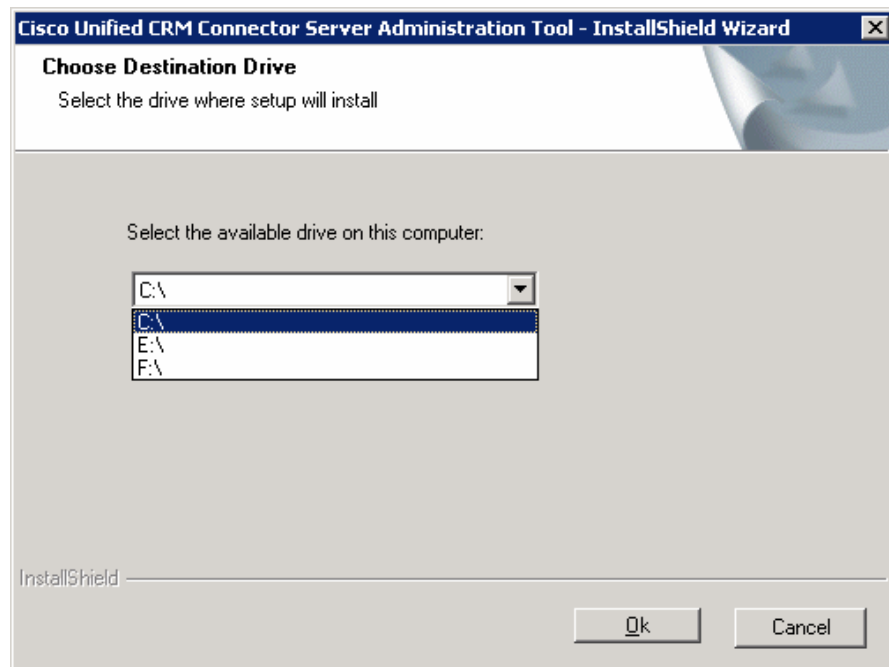


Step 3: Select the target installation drive.

- You are next prompted to select a drive location. The installer defaults to install the C: drive. The directory path is fixed, but you may specify the target drive. If you wish to change the drive, press the “Change Drive” button.” Otherwise continue by pressing Next.

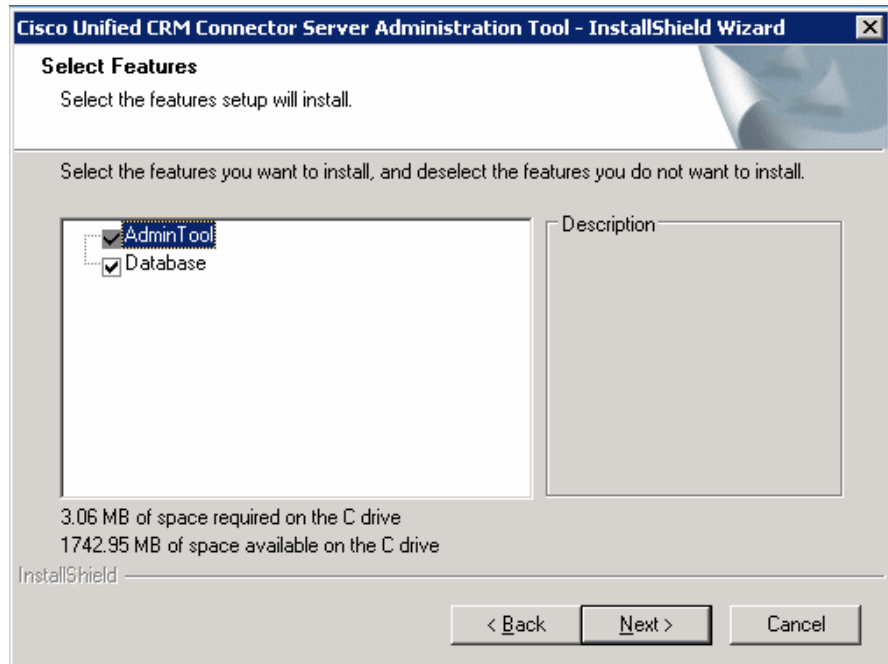


- Select the target drive. You may only install on a local drive, network mapped drives are not presented as a selection option.



Step 4: Select components to install.

- You may now choose which components of the Administration Tool to install.
 - You **must** install the Administration Tool.
 - If you are installing for the first time, install and configure the database components.
 - If you are re-installing or installing a redundant copy, do not install the database components.
- Press Next after making your selections.



Step 5: Configure the database settings (for first-time installs).

- Specify the Database Server location. This example shows the default for SQL Express on the local Administration Tool. If the SQL Server is running on another machine or as a production SQL Server instances, specify the machine name and the SQL Server instance name. The Browse option will identify Windows Servers and accessible SQL Server instances.
- Use the radio button to select the authentication method.
- If you select SQL Server authentication, you must specify the user account and password.
- Pressing Next begins the install.

- Press the Finish button to close the installation wizard.

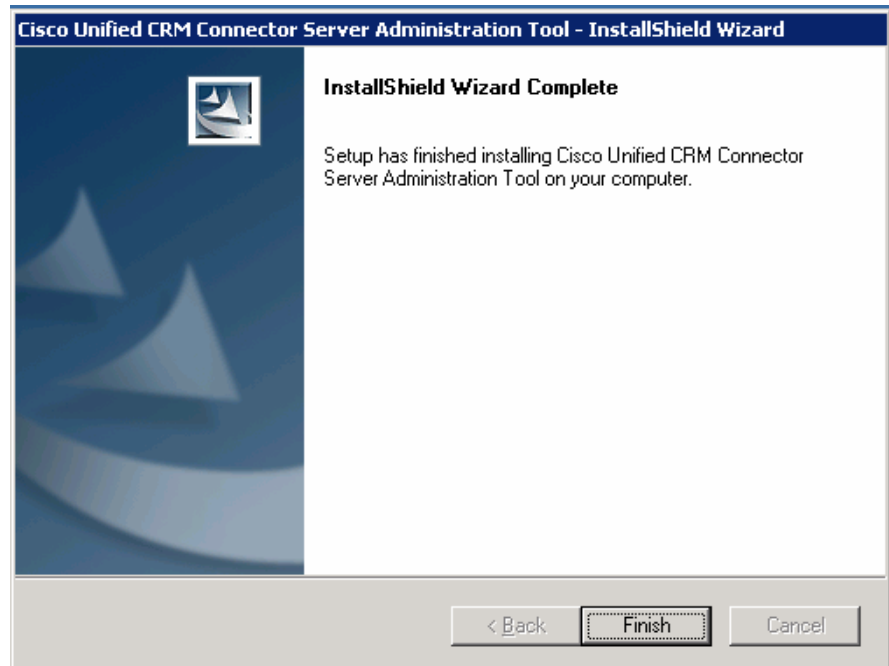


Table 4-1: Administration Tool Directory Structure

| Sub-Directory | Component | Use |
|---|------------|---|
| C:\Program Files\Cisco\CRM Connector | | This is the parent directory location; all administration tool components will be installed under this directory hierarchy. |
| C:\Program Files\Cisco\CRM Connector\Server Administration Tool | | This is the administration tool parent directory. All of the components are installed in subdirectories. Each subdirectory of the administration tool is used as a Virtual Directory under IIS. |
| ..\AdminToolWebService | | This is the directory structure for the administration tool web service. This services provides core functions to the Administration Tool You may need to change the settings to the web.config file in this subdirectory. |
| | Web.config | This file configures the web services and their execution capabilities. It includes configurations for running the web services. You should only change these configurations if directed by Cisco TAC. |

| Sub-Directory | Component | Use |
|-----------------------------|---|--|
| | ConversionReport.txt Global.asax.resx ManageMCIS.asmx ManageMCIS.asmx.resx MonitorMCIS.asmx MonitorMCIS.asmx.resx PrecompiledApp.config UpgradeLog.xml UpgradeLog2.xml | These are web services application files, resource files and system information files. |
| ..\AdminToolWebServices\bin | | This directory holds additional web services executables and configuration components. |
| | AdmintoolFactoryVB.dll AdmintoolFactoryVB.xml App_Code.compiled App_Code.dll App_global.asmas.compiled App_global.asax.dll Interop.ADMINTOOLSERVICELib.dll Interop.ADMINTOOLSERVICELib.reg | These files are dedicated to running the web services and should not be changed. |
| ..\CiscoAdminToolWebAppl | | This directory holds the application component of the Cisco CRM Connector Administration Tool; it forms a Virtual Directory running under IIS. |
| | Web.config | This file contains configuration settings, including access credentials for the SQL Server database that you will need to modify . |
| | AdminTool.css Admin_intro.html Calendar.aspx Calendar.aspx.resx CiscoAdminToolWebAppl.sln Default.aspx DesktopDefault.aspx DesktopModule.aspx DesktopPortalBanner.ascx Global.asax.resx MCISCallback.aspx MCISCallback.aspx.resx | These files are part of the administration tool and should not be modified. |

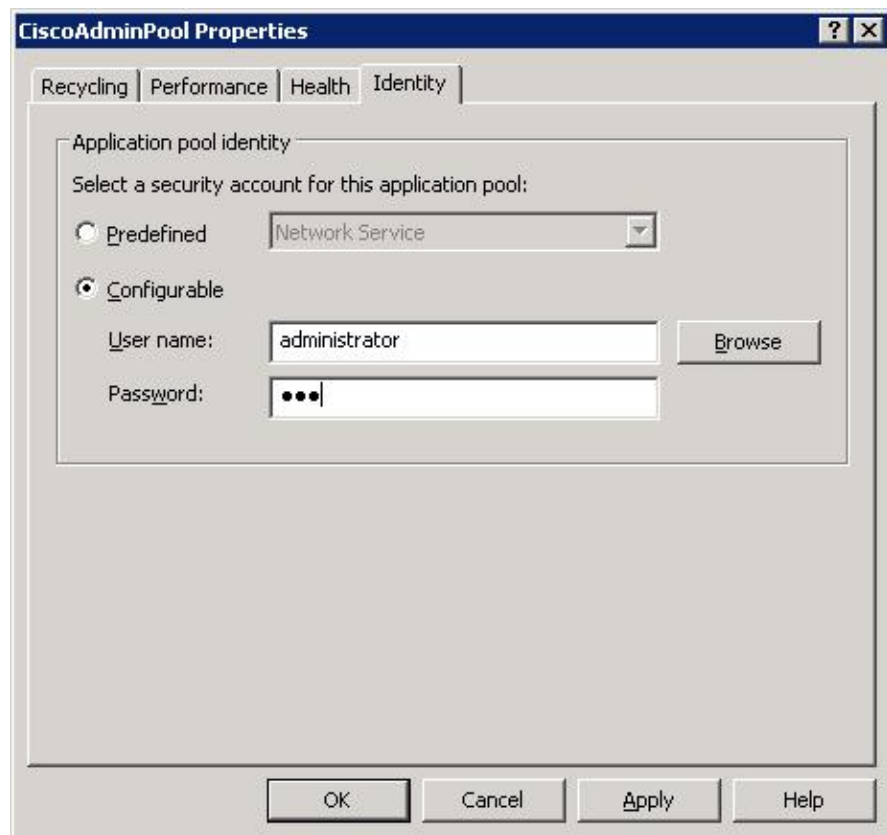
| Sub-Directory | Component | Use |
|---------------------------------------|--|--|
| | MCISCallback.js MCISModuleFooter.ascx MCISModuleTitle.ascx PortalCfg.xml PortalCfg.xsd PortalCfg.xsx PrecompiledApp.config Progress.js UpgradeLog.xml | |
| ..\CiscoAdminToolWebAppl\Admin | | This directory holds the application component of the Cisco CRM Connector Administration Tool; it forms a Virtual Directory running under IIS. |
| | accessdenied.aspx editaccessdenied.aspx 11/13/2007 09:45 AM <DIR> Images logoff.aspx manageusers.aspx moduledefinitions.aspx moduledefs.ascx modulesettings.aspx notimplemented.aspx Register.aspx roles.ascx securityroles.aspx sitesettings.ascx tablayout.aspx tabs.ascx users.ascx | These files are part of the administration tool and should not be modified. |
| ..\CiscoAdminToolWebAppl\Admin\Images | | This directory holds images used by the administration tool |
| | Admin_tool_header.jpg | This is an image file that displays in the administration tool header. |
| ..\CiscoAdminToolWebAppl\Admin\bin | | This directory holds executables and utilities used by the administration application web services components. |
| | App_Code.compiled App_Code.dll | These files are part of the administration tool and should |

| Sub-Directory | Component | Use |
|---|--|--|
| | App_global.asax.compiled App_global.asax.dll App_WebReferences.compiled App_WebReferences.dll App_Web_3ntdcnvs.dll App_Web_ggy_wkxp.dll | not be modified. |
| ..\CiscoAdminToolWebAppl\Admin\Components | | This directory is empty when installed. |
| ..\CiscoAdminToolWebAppl\Admin\DesktopModules | | This directory holds executables and utilities used by the administration application web services components. |

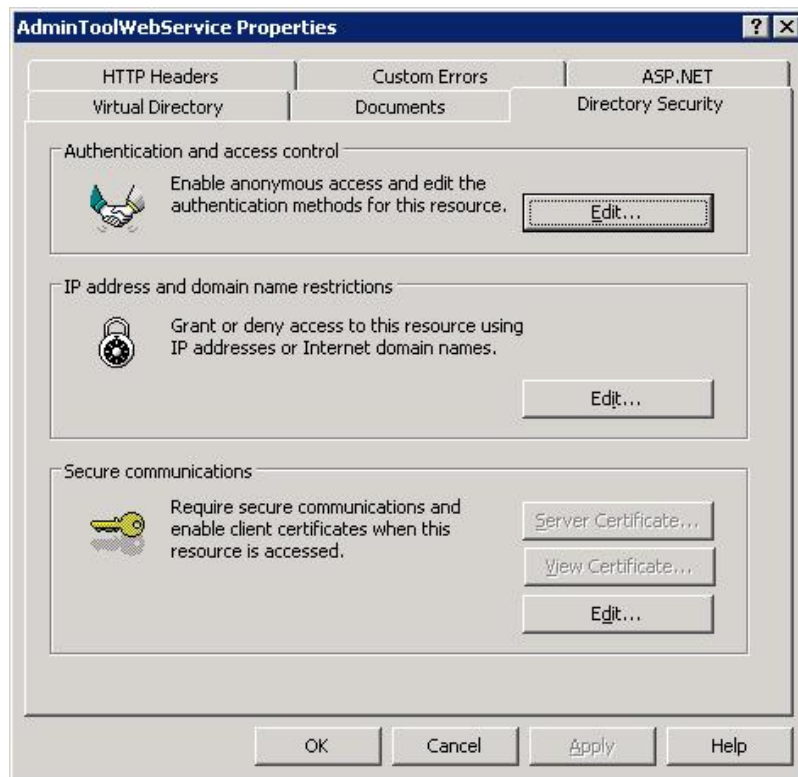
Configuring the Administration Tool

After installing the Administration tool you must modify the web services and web service configuration files to enable the Administration Tool.

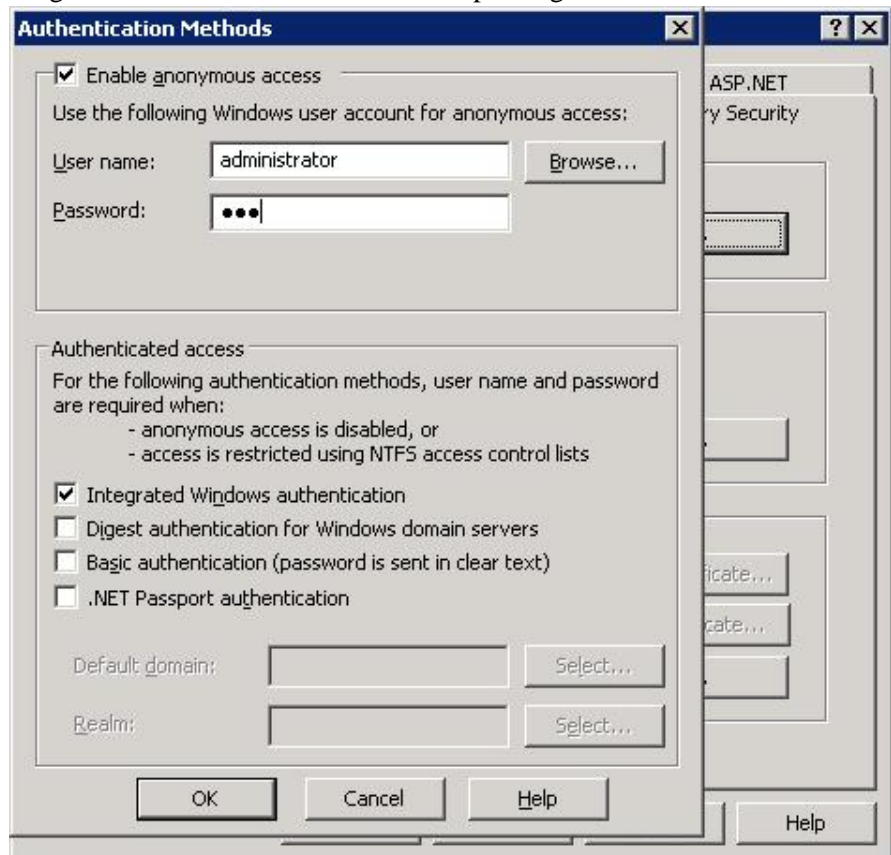
1. Select the CiscoAdminPool and assign the user account with local administration privileges on its properties identity tab.



2. Select the Directory Security tab to edit the Authentication and Access control settings: Click on the **Directory Security Tab**, then **Click on the Edit Button** to assign the user identity for the web service.

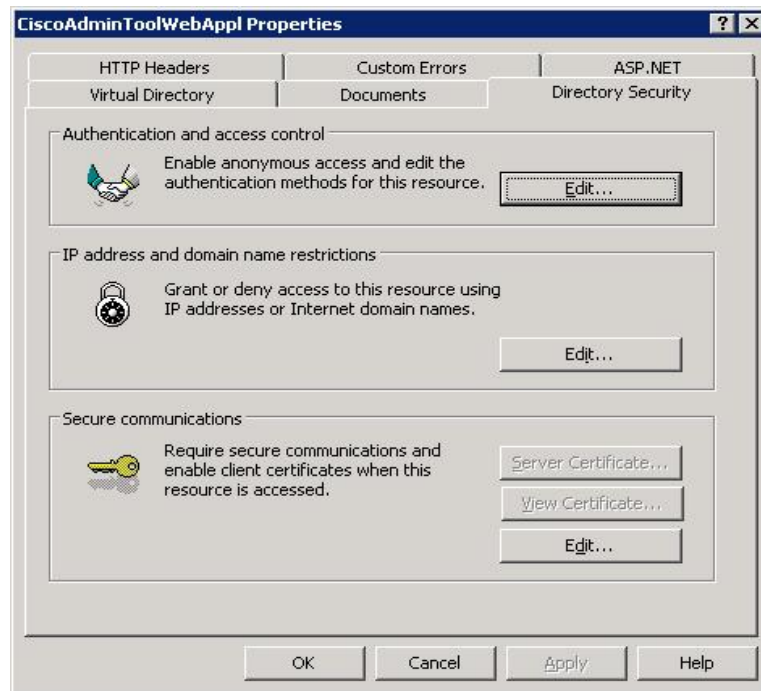


3. Assign the user with local administrator privileges.

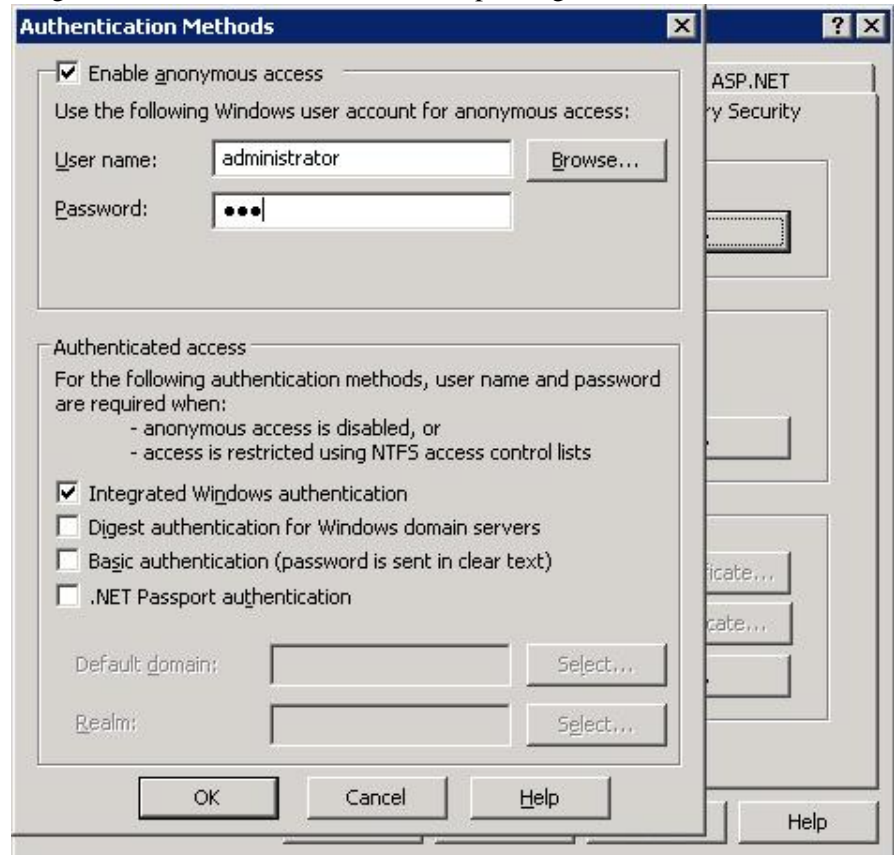


4. Click OK to save the changes to the AdministrationToolWebService.

Step 3: Verify and Assign the CiscoAdminToolWebAppl to the application pool and set the user identity and credentials.



1. Assign the user with local administrator privileges.



This completes the web application tool configuration activities.

Configuring the CRM Connector Server for the Administration Tool

In addition to the configuration of the Administration Tool settings you must change the configuration for each CRM Connector Server managed by the Administration Tool. This is configured in the CRM Connector Server *config.ini*, in the Administration Tool module section.

The Administration Tool does not require a Module Manager configuration. It runs independently, launched by web services and accesses the config.ini file independently, through the MCIS_INI environment variable.

Administration Tool Section

You must configure the Administration Tool section of the config.ini file so that the AdministrationToolService can connect with the web server and properly identify and manage the local CRM Connector Server. The required configuration keys, their valid values and their meaning and use are described in **Table 4-2: Administration Tool Configuration Keys**

Table 4-2: Administration Tool Configuration Keys

| Key | Valid Values – Meaning | Meaning / Use |
|----------------|---|--|
| TracePath | <p>Directory path name only: do not include the file name. This path must end in a back slash “\”</p> <p>Note: If you do not add the trailing backslash, the TraceFileName will merge with the last directory name to form the file name and the file will be in the parent directory.</p> <p>Example: TracePath=c:\A\B TracefileName=hello.txt Will become c:\A\Bhello.txt.</p> | <p>The directory path where the Administration Tool log files will be saved and accessed.</p> <p>Note: this is only the path; do not include the log file name here.</p> |
| TracefileName | A valid windows file name; this should end in “.log” so that it can be accessed by the Administration Tool log reader. | This is the name of the trace file for the Administration Tool. The default name is “AdministrationTool.log” you should not change it. |
| AdminToolHost | Host name or IP Address | The host name or IP address of the server running the AdminTool service. This is the name of the Administration Tool server, not the name (or IP address) of the CRM Connector Server. |
| WebServiceHost | Host name or IP Address | The host name or IP address of the IIS server running the web services. |

| | | |
|-------------------|---|---|
| MCISName | A unique name for the CRM Connector Server. | This is a unique name used to display the CRM Connector Server in the administration tool. It is a required configuration value. Select a meaningful name which should not be assigned to another CRM Connector Server. |
| AdminRemotingPort | A valid port address. If there is a firewall between the web services (WebServiceHost) and the CRM Connector Server this port must be opened in the firewall. NOTE: If you change this value you must also update the web service web.config file, change the port number. | The port address for communicating between the CRM Connector Server and the web services on IIS. The default value of this is 65372. |

Using the Administration Tool Implementation

Once the Administration Tool is installed and configured, you may use it to manage any CRM Connector Server in your environment. You must be sure to follow the steps above in Configuring the Administration Tool for the CRM Connector Server.

Use the administration tool to manage your CRM Connector Servers: to start, stop or restart them, to change configurations and apply licenses. This section explains how to administer the Administration Tool itself and how to use it to manager your CRM Connector Servers.

Accessing and logging into the Administration Tool

Use the Microsoft Internet Explorer (IE) browser to run the Administration Tool.

Step 1: Accessing the Administration Tool

You may access the Administration Tool from any machine in your organization; just enter the URL for the web services IIS it is implemented upon.

Accessing from the “local” machine – the IIS server.

If you run it from the IIS server you would enter this URL:

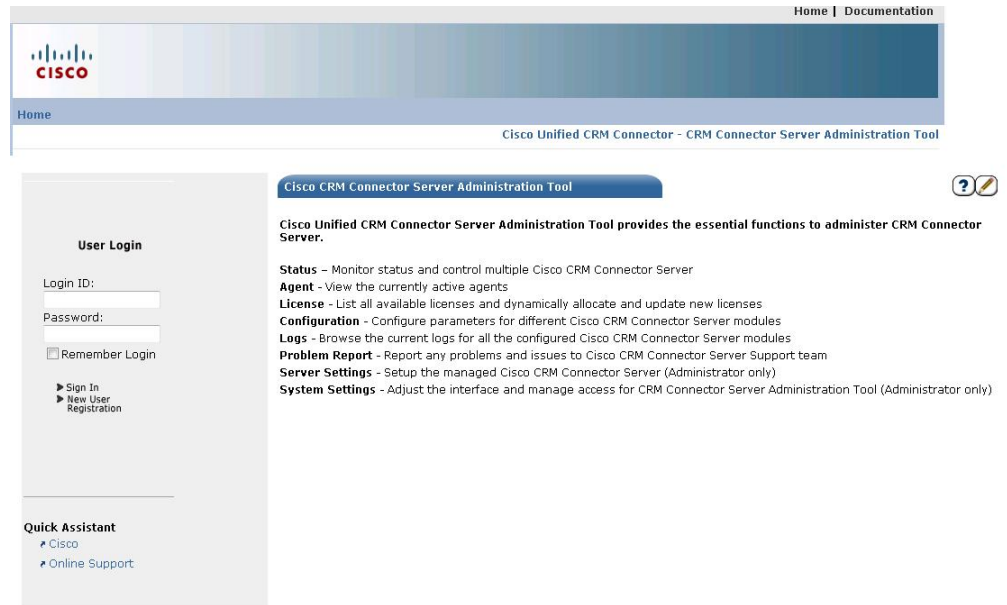
http://localhost/CiscoAdminToolWebAppl

Accessing from a remote client.

To access the Administration Tool from a remote client, simply substitute the server name for the “localhost” in the URL above. E.g., if you your IIS server is “IISHOST” then use this URL to access the Administration Tool: **http://IISHOST/CiscoAdminToolWebAppl**

This launches the Administration Tool home page (Figure 4-1: Administration Tool Home Page).

Figure 4-1: Administration Tool Home Page



Step 2: Logging In

You must log in to start a session before performing any activities. To log into the Administration Tool for the first time, use this user account:

Login ID: **super**

Password: **guest**

You will then be authenticated and a navigation menu will be enabled with all valid options above just below the Cisco banner (Figure 4-2: User Logged In)

Figure 4-2: User Logged In



WARNING: You should now immediately change the super user's password since anyone accessing this account will have full administrative control.

Figure 4-3: New User Registration Form

The screenshot shows the 'New User Registration Form' within the 'Cisco Unified CRM Connector - CRM Connector Server Administration Tool'. The form is titled 'Create a New Account' and includes the following fields:

- Name:** Michael Smyth
- Login ID:** msmyth
- Password:** (masked with dots)
- Confirm Password:** (masked with dots)
- Telephone:** +1 (703) 555-1212
- Email:** msmyth@mycompany.com
- Company Information:** A text box containing the placeholder text 'Comments about who I am and how I use the Connector Server Administration Tool.'

At the bottom of the form, there is a blue link labeled 'Register and Sign In Now'.

Registering a New User

Each user of the administration tool may have their own account, and the super user (or any administration privileged account) may be used to grant access to menus.

New users may register by opening the home page (Figure 4-1: Administration Tool Home Page) and clicking the “New User Registration” link.

This brings up a registration form where new users may create their account name and set a password. Figure 4-3: New User Registration Form shows the filled in registration form.

Users should enter their name, the desired login id and password, as well as contact information, phone number and e-mail address. For large companies some description of the user’s role is useful in the Company comment text box. Clicking the [Register and Sign In Now](#) link completes the registration and logs in the user.

After registering, the new user will have no privileges: none of the menu options will be accessible to them. An administrator must grant their user rights. This process is explained in the next section.

Granting User Rights

Any user with administrative privileges may grant access rights to a new user. Here are the steps to follow:

STEP 1: Open the Systems Settings Page.

Click on the Systems Settings menu option. This launches the System Settings page as shown in Figure 4-4: System Settings Page.

Figure 4-4: System Settings Page

CISCO

Home Status Agent License Configuration Logs Server Settings **System Settings**

Cisco Unified CRM Connector - CRM Connector Server Administration Tool

Site Title: Cisco Unified CRM Connector - CRM Cor

Always show edit button?: ☐

[Apply Changes](#)

[Add New Tab](#)

Tabs: Home Status Agent License Configuration

Move selected tab up in list

Admins

Manager

[Add New Role](#)

Domain users do not need to be registered to access portal content that is available to "All Users". Administrators may add domain users to specific roles using the Security Roles function above. This section permits Administrators to manage users and their security roles directly.

Registered Users: **msmyth** [Add New User](#)

STEP 2: Assign the Registered User to the Role.

1. Select the registered user from the "Registered User" drop down.
(Highlighted with the red box in Figure 4-4: System Settings Page.)

Figure 4-5: Registered User Authentication Page

Welcome super! | Home | Documentation | Logoff

CISCO

Cisco Unified CRM Connector - CRM Connector Server Administration Tool

User: msmyth

Password:

Confirm Password:

Telephone: +1 (703) 555-1212

Email: msmyth@mycompany.com

Company Information:

Comments about who I am and how I use the Connector Server Administration Tool.

[Apply Changes](#)

Admins [add user to this role](#)

Admins

Manager

[Save User Changes](#)

2. Click on the pencil icon to the right of the Registered User drop down.
This launches the edit user page shown Figure 4-5: Registered User Authentication Page.

3. You may assign the user a privilege role using the “Add user to role” drop down, at the bottom of the authentication page. Select a role from the drop down; two roles are pre-configured “Admins” grants full administration rights and “Manager” grants more limited control rights.

STEP 3 (Optional): Correct any user contact information.

You may also change any user settings, their contact information, etc from this page and the user’s password.

STEP 4: Save the Changes

Press the “[Save User Changes](#)” link to save the role changes and any other changes you have made to the user configuration.

The newly assigned user role will appear below the “Add user to this role” selection and the user will now be able to log in with the assigned role and its privileges.

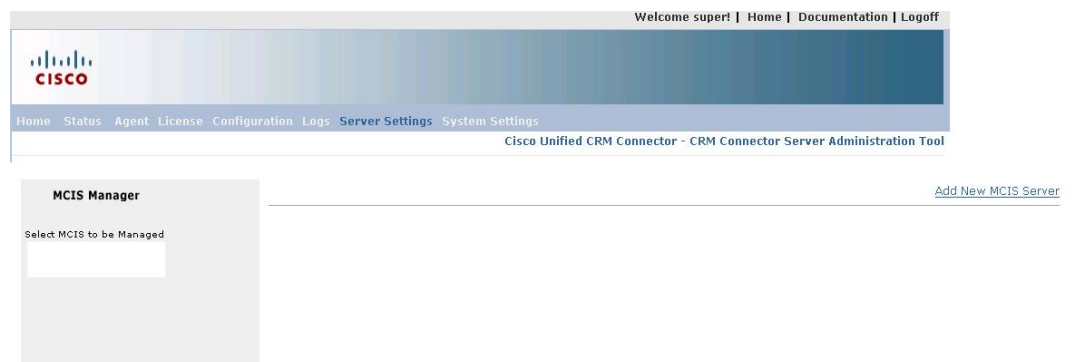
Adding a CRM Connector Server

In order to manage a CRM Connector Server (here referred to by its project name “MCIS,” which stands for multi-channel information server) you must add it into the Administration Tool. Adding the CRM Connector Server maps its name (the MCISName) and address (host name or IP address and port) with the CRM Connector Server: these are the same values entered into the server’s configuration file (config.ini).

STEP 1: Navigate to the System Settings Page

The System Settings page lets you associate a CRM Connector Server within the Administration Tool, as well as change or delete existing associations. Figure 4-6: Server Settings Page shows the initial page, with no servers associated.

Figure 4-6: Server Settings Page



STEP 2: Add the Server settings.

To add a server, press the “[Add New MCIS Server](#)” link; this will navigate to the server settings entry page (Figure 4-7: Server Setting Entry Page).

This prompts for three entries:

- **MCIS Name:** Enter the CRM Connector Server name as it was entered in the AdministrationTool section of the server's **config.ini**.
- **Server Name:** This is the host name for the CRM Connector Server, or you may enter the IP address if you do not use DNS names.
- **IP Address:** This is the IP address for the CRM Connector Server.

Figure 4-7: Server Setting Entry Page

Welcome super! | Home | Documentation | Logoff

CISCO

Home Status Agent License Configuration Logs Server Settings System Settings

Cisco Unified CRM Connector - CRM Connector Server Administration Tool

| | |
|--------------|---------------|
| MCIS Name: | CRMTest |
| Server Name: | cscrmtest |
| IP Address: | 192.160.0.242 |

[Update](#) [Cancel](#) [Delete this item](#)

STEP 3: Save the Settings

Press the “[Update](#)” link to save the settings. This will navigate back to the System Settings page, which now will display the associated CRM Connector Server. Figure 4-7: Server Setting Entry Page shows the entered server information. The name of each server appears in the MCIS Manager box on the left side of the page.

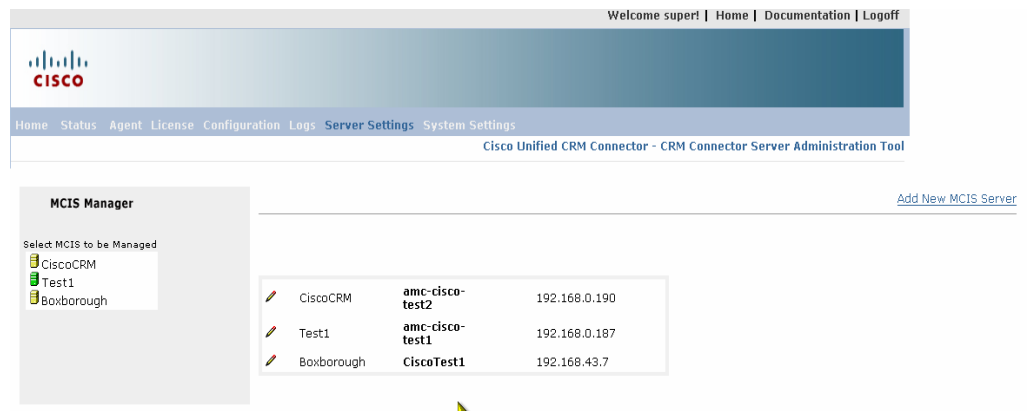
If you manage more than one server, select the server to manage by clicking its entry in the MCIS Manager box. The selected server is highlighted in yellow. The server icon color identifies the current state. If the Administration Tool cannot connect with the server it will remain gray. If the Administration Tool can connect with the server, the icon will either be red or green:

- **RED:** The server is not started
- **GREEN:** The server is started
- **GREY:** The Administration Tool cannot connect with the server.

The right column lists each associated server. You may edit a server by clicking on the pencil icon to the left of the server name.

Note: There is no need to select a server before editing it. Selection is used to determine the managed server on the Status, License, Configuration and Logs pages.

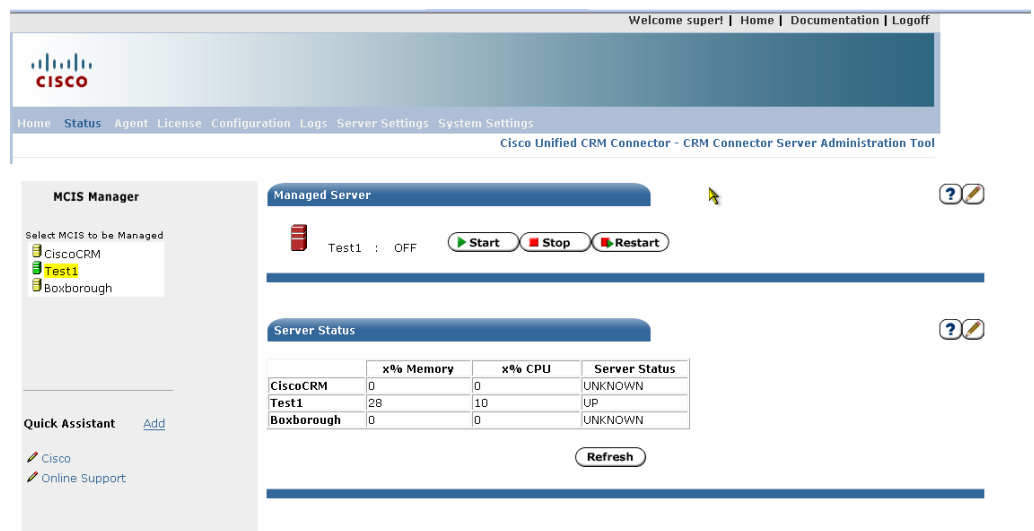
Figure 4-8: System Settings w/ Servers Added



Monitoring and Controlling Server Status

You may monitor and control your servers' status through the Status page. Click on the "Status" link in the menu line to navigate to the Server Status page. Error! Reference source not found. shows the Server status page. CRM Connector Server Test1 is stopped. As with all pages, the Server Manager column on the left allows you to select the server to manage.

Figure 4-9: Server Status with Stopped Server



The center column shows the server status and is divided into two parts. The upper part provides controls that enable you to start, stop, or restart the selected server. The lower part shows the selected server's resource utilization.

START a server.

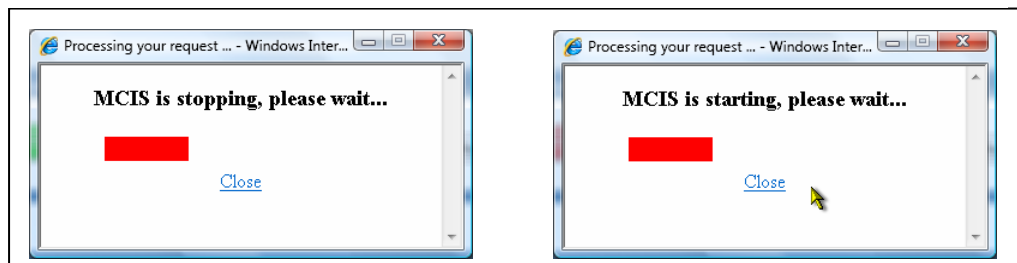
You may start a stopped server. Stopped servers will display a RED server icon in the Manager column.

To start a server, select the server from the Manager column; this will highlight the server in yellow and list the server in the center column. Press the **START** button.

This will send a start message to the server and open a small progress window. When the server has started the progress window will close, the server status page will repaint and the new server status will show as a GREEN icon in the Manager and center column. Figure 4-10: Server Start and Stop Progress Bars shows the progress message boxes.

STOP a server.

Figure 4-10: Server Start and Stop Progress Bars



To stop a server, select a started server and press the STOP button. This will display the server status progress window. When the server stops, the window will close and the server icon will revert to red as shown in Figure 4-9: Server Status with Stopped Server.

RESTART a server

Certain server management changes require restarting the server: for example when changing a configuration you must restart the server to apply the change. Press the RESTART button to restart the server. The small progress window will open while the server restarts. If the restart is successful it will display the server icon in GREEN and the current resource utilization.

Licensing a Server

You must license each CRM Connector Server. The licenses are issued based on the number of users who will connect with the server. Your partner vendor or systems integrator will provide you with the license keys. This section describes how to work with your partner vendor to acquire the licenses and then apply them.

The Licensing Process

To license a server you must first generate a registration key, this is a license seed key that uniquely identifies a single CRM Connector Server and is used to generate the licenses exclusively for that server. Generate the key using the Administration Tool license page and provide this key to your Cisco partner vendor who will use it to generate the licenses for your server.

Your Cisco partner will provide you with the licenses for your system. Each CRM Connector Server requires three licenses:

- MCIS: These are server licenses.
- CTI_Cisco: These are the connector licenses.

- AA-DOTNET: These are the .NET adapter licenses.

Use the license page to apply your licenses; or you may simply enter them into the config.ini on the CRM Connector Server using a standard editor.

The License Page

The license page is used to monitor licenses assigned to a server, to generate the license registration key and to apply licenses and record them in the config.ini file on the CRM Connector Server.

The left side column Manager section allows you to select a server. Many of the licensing actions require the server to be started, so you should start the server if it is stopped.

Selecting a server displays its assigned licenses and allows you to generate the registration key, enter and apply the license and validate the applied license for a running server.

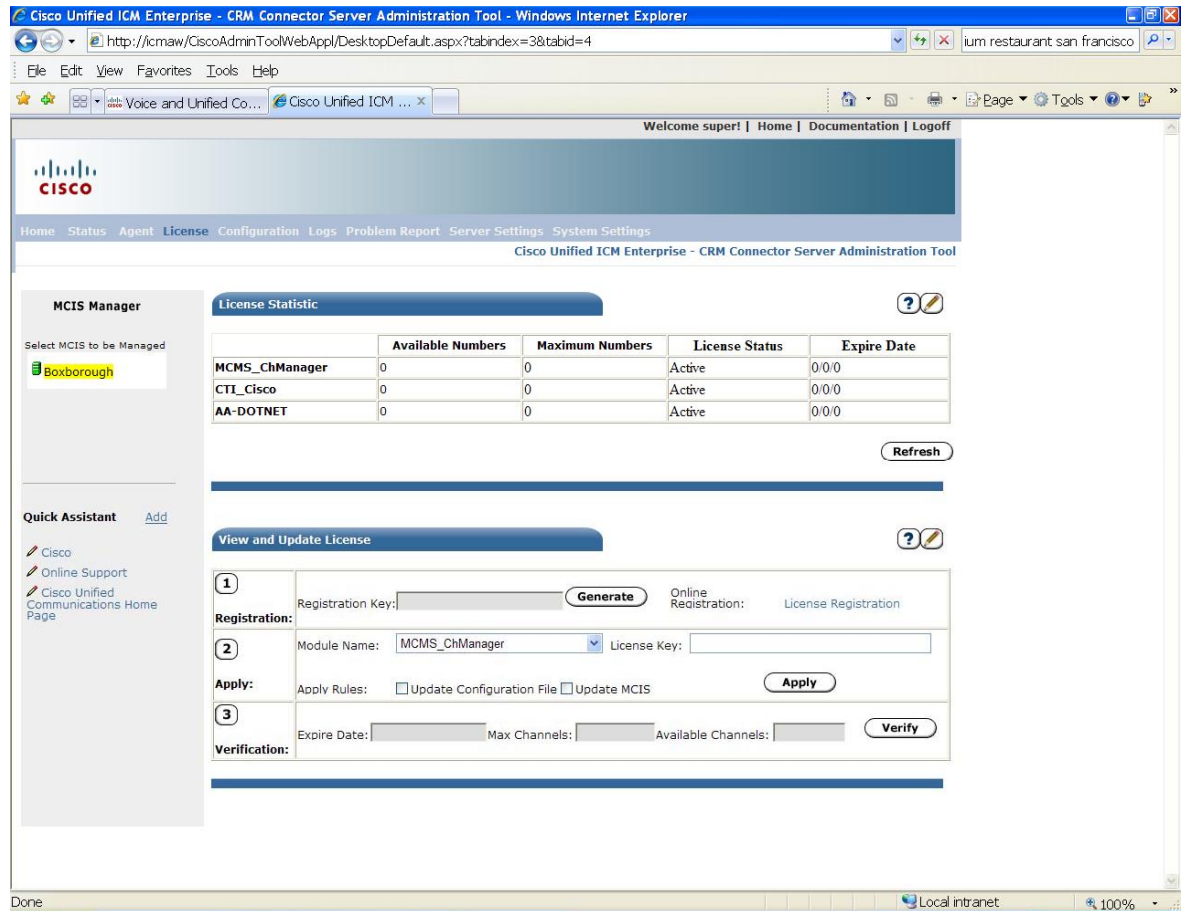
The top section of the middle column shows the assigned licenses. Each license type has a single line with five columns:

- First column: this displays the license type for the display line.
- Available Numbers: this displays the total available licenses for each license type. The available number indicates how many more agents may log into the server.

Note: there is only one license assigned to the AA-DOTNET adapter, when running it will normally show zero (0) available licenses.

- Maximum Numbers: this displays the total number of licenses, which equates to the total number of agents the server will support.
- License Status: this shows the license status. Valid, permanent licenses will always show ACTIVE. If a license has expired or is invalid it will show INACTIVE.
- Expire Date: this shows the expiration date for temporary licenses. Licenses will show PERMANENT in this column.

Figure 4-11: License Page



The lower section of the license page provides a three step action sequence that allows you to generate and apply licenses.

Step 1: Generate The Registration Key.

To generate the registration key, navigate to the license page and select the CRM Connector Server.

In the lower section, under Step 1: Registration, press the Generate key. This will generate a unique registration key and display it in the Registration Key text box.

Highlight and copy the Registration Key and send it to your partner vendor.

Note: if you have more than one CRM Connector Server you should be sure to note the server name so as not to confuse registration keys. There is one and only one Registration Key per server.

Figure 4-12: Generate License Key shows the generated registration key.

Figure 4-12: Generate License Key

The screenshot displays the Cisco Unified CRM Connector - CRM Connector Server Administration Tool interface. The top navigation bar includes links for Home, Status, Agent, License, Configuration, Logs, Server Settings, and System Settings. The main content area is divided into two sections: 'License Statistic' and 'View and Update License'.

License Statistic

| Available Numbers | Maximum Numbers | License Status | Expire Date |
|-------------------|-----------------|----------------|-------------|
|-------------------|-----------------|----------------|-------------|

View and Update License

1. Registration: Registration Key: WADMCMVDRQ0000J Generate Online Registration: License Registration

2. Module Name: MCIS License Key: Apply Rules: ☐ Update Configuration File ☐ Update MCIS Apply

3. Verification: Expire Date: Max Channels: Available Channels: Verify

Step 2: Apply the License

In Step 2 you may update the configuration file with the new license keys. You may also apply the license keys in real-time, without restarting your CRM Connector Server.

Your Cisco vendor will provide you with the licenses and note the license type.

In the Step 2 area, use the drop down to select the license type. Copy and paste the provided license key into the License Key text box.

Select whether you wish to record the licenses or apply them in real-time or both. To update the configuration file and record the licenses, check the **“Update Configuration File”** check box. To apply the licenses to the running server without restarting, check the **“Update MCIS”** checkbox.

Press the Apply button. This will apply the licenses and re-paint the page.

If you chose to apply the licenses to the running server, the license status section of the License Page will update to show the current assigned licenses.

Note: When applying the license, the administration tool displays a warning dialog informing you that the new licenses will overwrite the current licenses. You must respond “OK” to this dialog to apply the licenses. Figure 4-13: License Application Warning shows the warning dialog.

Repeat this for each license.

Note: You do not need to generate a new registration key when applying the licenses. The registration key is used by Cisco as a “seed” to generate all licenses for each CRM Connector Server.

Figure 4-13: License Application Warning



Step 3: Verification

In Step 3 you verify the license key. Once the license key is entered into the configuration file or applied to the running CRM Connector Server, you should ensure that you have entered it correctly.

Press the “Verify” button in step three. This will check the licenses and return the license information. If the licenses are not valid they will show incorrect information here or will show no available licenses.

To verify a license:

- Select the CRM Connector Server.
- Select the license type (in the drop down box under Step 2).
- Press the verify button.

If the license is valid, correct license information will display in the three text box displays:

- Expiration Date should show PERMANENT.
- Maximum Channels will show the correct total number of licenses.
- Available Channels will show the total available channels: maximum channels less the total number of active users (or consumed licenses).

Managing Configuration File

The Administration Tool can access, display and modify the configuration files from remote CRM Connector Servers. This easily allows you to view or modify configuration settings without opening the configuration file into an editor.

Select the “[Configuration](#)” link from the menu line to navigate to the configuration file edit page. On this page you may open, view and edit the full configuration file or you may edit a configuration file section.

Note: In order to manage configuration files through the configuration page you **must** name your current configuration file “config.ini.” All other configuration files are assumed to be backup files.

The configuration page is divided into three parts:

- The “Configuration Template” displays the loaded configuration file or file section. You may view, scroll and edit the configuration file within this section.

- The Current Configuration Section. This allows you to read the current configuration file (config.ini) OR a specific module section into the Configuration Template area for viewing and editing.
- The backup configuration section. This allows you to manage backed up configuration files: create or name a backup configuration, open a configuration backup and promote a backup to be the current configuration file.

Edit a Module Section

The “Modules” section allows you to read in and save out the current configuration file or a select configuration module section.

- Select a configuration file section: use the “Modules” drop down, which lists all modules in the current configuration file, to select a specific section by name.
- Use the “Read Section” button to read the selected section into the Configuration Template.
- Edit the section within the Configuration Template area.
- Use the “Save Section” to save modifications from the Configuration Template.

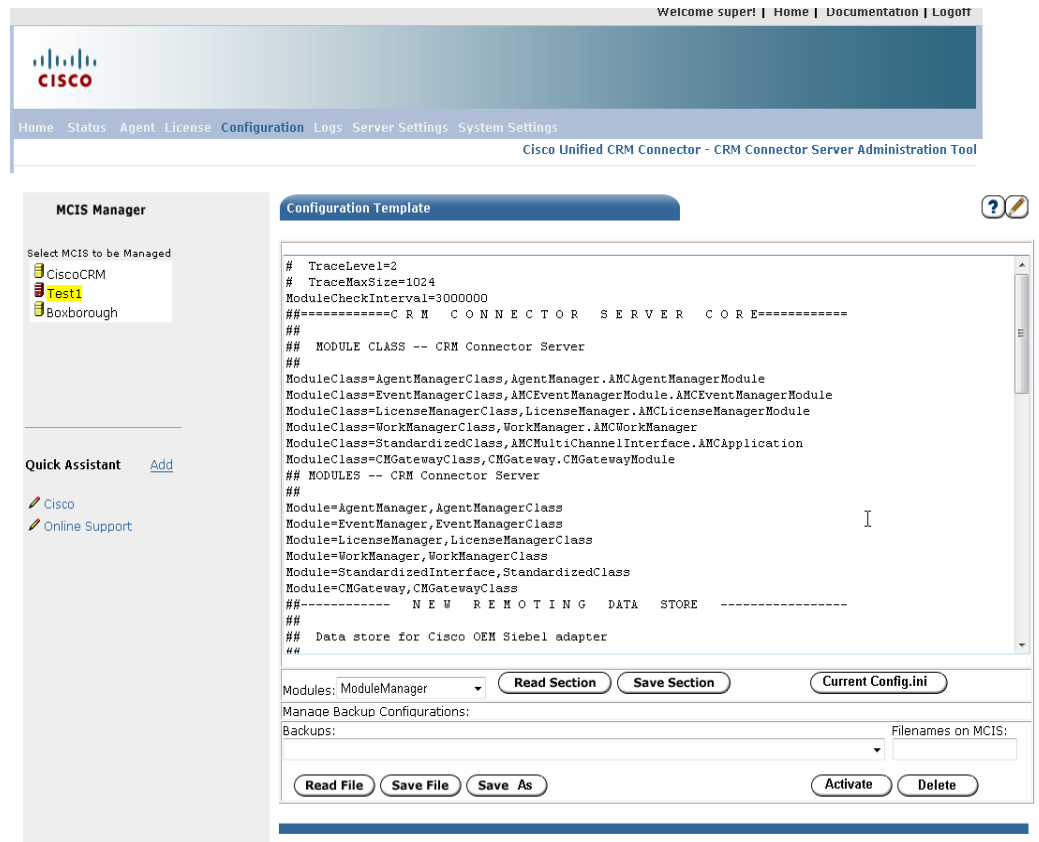
Edit the Full Configuration File

- Use the “Current Configuration” button to read in the current configuration file.
- Edit the section within the Configuration Template area.
- Use the “Save Section” to save modifications from the Configuration Template.

Working with Configuration Backups

The last section “Manage Backup Configurations” allows you to open backup files into the viewer and editor, save changes with a new file name or promote backup files to become the current configuration file.

Figure 4-14: Configuration Edit Page



Editing a Backup File

All configuration backup files, those in the configuration directory ending in **“.ini”** are listed in the backup file drop down.

- Open and read a backup configuration file. All files in the configuration directory ending in **“INI”** are listed in the backup file drop down. Select the file name and use the **“Read File”** button to read the file into the configuration area.
- Edit the configuration settings in the viewer / editor.
- Save changes. Use the **“Save File”** button to save changes.

Saving the Configuration Settings to a different file.

There is no way of renaming a configuration file. However you may save the current editor / viewer contents to a different file name.

- Enter the new file name in the **“File Names on MCIS”** text box.
- Use the **“Save As”** button to save the current editor / viewer contents to the newly named file.

Warning: If you select the same name as a current file and press the “Save As” button you will receive a warning dialog that this will over-write an existing file.

Activating a Configuration File

Activating a configuration file promotes it from a backup to the current configuration file; this also backs up the current configuration file.

- Select a backup configuration from the drop down.
- Use the “Activate” button to activate the selected configuration file and backup the current configuration file.
- You must re-start the CRM Connector Server (from the Status page) in order to complete the activation.

Deleting a Configuration File

Deleting a configuration delete the configuration file.

- Select the backup configuration to delete from the drop down.
- Use the “Delete” button to delete he backup configuration.

Managing Logging

The Administration Tool allows you to change the current active trace level for logging, either globally or for a specific module, and to view the current log files for specific modules Figure 4-15: Trace Control and Log File Viewing Page shows the log management page. Navigate to this page by clicking the “[Log](#)” link on the menu line.

Figure 4-15: Trace Control and Log File Viewing Page

Welcome super! | Home | Documentation | Logoff

CISCO

Home Status Agent License Configuration Logs Server Settings System Settings

Cisco Unified CRM Connector - CRM Connector Server Administration Tool

MCIS Manager

Select MCIS to be Managed

- CiscoCRM
- Test1
- Boxborough

Quick Assistant Add

- Cisco
- Online Support

Trace Level

Current Global Trace Level: Errors+Warnings+Info **Read** Trace Level: Errors **Save**

Module List: Global Trace Level: Set Trace Level: Errors **Save**

Log Viewer

Module: DataStore Filter Rule: All **View**

Time: BETWEEN AND Current Page: 0

DataStore.log(1/25/2008 9:50:56 AM)

```
I20080125-092010.783,2236, 0,Initialized Tracing for Module 'DataStore'
D20080125-092010.783,2236, 0,Base Initialization for Module 'DataStore' returning 0x0
D20080125-092015.933,2236, 0,Base Start for Module 'DataStore' returning 0x0
I20080125-092015.953,3856, 0,DataCleanupThread: Start (CleanupInterval = 300000 ms) >>>
I20080125-092524.522,3856, 0,Checking for expired data (#1)...
I20080125-092524.532,3856, 0,Done with checking #1 (0 cleaned)
D20080125-092854.464,2236, 0,Base Stop for Module 'DataStore' returning 0x0
```

Trace Level Section Described

You may temporarily change the trace level for logging using the Trace Level section of the Log management page. This section is divided into two parts:

- The global trace level section. This section allows you to retrieve the current global trace level settings and to change them.
- The module trace level section. This section allows you to retrieve and change the trace levels for a specific module. Use this if you encounter a problem in a specific area, such as upon a specific CRM Connector configuration, to set its trace level.

Viewing and Changing the Global Trace Level

The global trace level section allows you to view and change the global trace settings. Use this if you **do not** override trace levels by module. It will only affect trace levels that are not set within the module sections.

Use the Log Control Page to perform these two functions:

- To read the current global configuration setting.
 - Use the “Read” button in the global configuration area to the right of the “Current Global Trace Level” textbox.

- This will populate the text file with the current global configuration setting. It is grayed out because you cannot edit this setting.
- To change the global trace level setting.
 - Select the trace level from the “Trace Level” drop down. You may choose from the following trace levels:
 - Errors – this will record errors only in the trace files.
 - Errors + Warnings – this will record all errors and any warnings in the log files.
 - Errors + Warnings + Info – this will record information entries as well as errors and warnings.
 - Errors + Warnings + Info + Debug – this adds debug information to errors, warnings and info entries.
 - Customized (Not Default) Tracking – this enables a customized logging level.
 - Press the “Save” button to apply the changes.

Note: When the CRM Connector Server restarts it will revert to the trace level settings in the global section of the config.ini file. This only “saves” these as the current setting and does not make these changes permanent, that requires changing the configuration file.

Viewing and Changing Module Trace Levels

The Trace Level module section allows you to view and change the trace level for individual modules. These changes only apply until changed or the CRM Connector Server restarts.

- Viewing the trace level for a module. You may view the trace level for any module and then will have the option of changing the module’s trace level.
 - Select the module from the drop down “Module List” drop down. All defined modules for the current configuration file are listed in this drop down.
 - After selecting the module the Log information file page will repaint and display the current trace level settings in the “Trace Level” text box to the right of the drop down. The trace level will be grayed out because you cannot edit this text box.
- Changing the trace level for a module. You may change the trace level for any module. This change will apply until you change it again or until the CRM Connector Server restarts.
 - Select the module from the “Module List” drop down.

- Use the “Set Trace Level” drop down to select a new trace level. There are five trace levels you may apply:
 - Errors – this will record errors only in the trace files.
 - Errors + Warnings – this will record all errors and any warnings in the log files.
 - Errors + Warnings + Info – this will record information entries as well as errors and warnings.
 - Errors + Warnings + Info + Debug – this adds debug information to errors, warnings and info entries.
 - Customized (Not Default) Tracking – this enables a customized logging level.
- Press the “Save” button to apply the change.

Note: When the CRM Connector Server restarts it will revert to the trace level settings in the global section of the config.ini file. This only “saves” these as the current setting and does not make these changes permanent, that requires changing the configuration file.

Viewing Current Log Files

Use the “Log Viewer” section to select modules and view the current log files. You may filter the log file to view only certain classes of log entries, e.g., all log entries, or warnings only, etc. You may also specify a time range to view log files for a defined period. Some large log files may run for two or more pages.

To view and filter the log file entries for a module:

- Use the “Module” drop down to select which module’s log entries to view. This drop down will list all currently running modules.
- Use the “Filter Rule” drop down to set and apply a filter rule. There are five (5) filter rules:
 - All
 - Only Errors
 - Only Warning
 - Only Debug
 - Only Others
- Use the “Time” entries, to specify a closed or open ended date range.
 - Enter a start date in the “Between” text box or use the calendar button to the right of the text box to open the calendar control and select a start date for the date range.

- You may enter an end date to close the date range by entering a date in the “And” text box (or use the calendar control) For an open-ended range, leave this box empty.
- Press the “View” button to open the log file and populate the view section.
 - This will display the log file name and the last update date and time in a line above the log file viewer.
 - The viewer displays the log file entries.
 - Large log files may be broken across two or more pages. Use the Page buttons in the filter selection area to advance or backup pages.

5. IMPLEMENTING THE CRM CONNECTOR

Purpose

This chapter describes how to configure the CRM Connector to integrate with the Cisco Unified ICM and Unified Contact Center Enterprise and Hosted through the CTI Server. You must integrate with at least one Cisco peripheral.

For Unified Contact Center Enterprise and Hosted implementations there is usually only one connector implementation for your enterprise. For Unified ICM you will need to implement one connector per peripheral (legacy switch).

This chapter covers:

- Pre-Requisite Installs
- Configuring CMR Connector for Unified Contact Center Enterprise and Hosted.
- Configuring CRM Connector for Unified ICM single sites
- Configuring CRM Connector for Unified ICM multi-sites
- Testing CRM Connector implementations

Before you begin

Before installing the CRM Connector software the CRM Connector Server must be implemented: installed, configured and tested. You should also have already implemented the CRM Connector Server Administration Tool.

Installing the CRM Connector Software

There is no special install step for the CRM Connector Software. It is installed as part of the CRM Connector Server installation. The installation included the directory structure shown in Table 5-1: CRM Connector Component Directory Structure.

Table 5-1: CRM Connector Component Directory Structure

| Sub-Directory | Component | Use |
|-------------------------------|---------------|---|
|\Cisco\CRM Connector\MCIS | | Core services parent sub-directory. The configuration files, the core service executables and DLLs, and the log files are under this sub-directory. |
| | Config.ini | Configuration file. |
| ... \Connectors\Cisco ICM | | Connector Sub-Directory Tree with the Cisco CRM Connector for UICM, UCCE, and UCCH sub-directory |
| | Cisco_ICM.dll | The CRM Connector module component |
| | Ati80.dll | Supporting software for the CRM Connector |

That reduces this implementation to a simple configuration to meet your Cisco Unified Contact Center environment. There are two significant Cisco Unified Contact Center environment classes.

The first is built upon Cisco Call Manager and consists of a single site enterprise scale implementation. The Expert Agent PG that supports Call Manager treats it as a single peripheral and therefore as a single site. A multi-site configuration of Unified Contact Center involves multiple implementations of Unified Contact Center Enterprise and Hosted. This would be implemented using multiple CRM Connector Servers and therefore is really two separate implementations.

Note: This simplifies the implementation to cover 90% of the likely implementations. It is possible to configure multiple instances of the CRM Connector for UCCE and UCCH. Simply create multiple instances of the CTI connector and configure each CTIModule with a different name.

The second implementation class is built upon the Unified Intelligent Call Manager. Implementing Unified ICM is more likely to involve multi-site implementations because it presents a more complex integration topology. Unified ICM integrates third-party ACDs (switches) through a dedicated peripheral type; there is a PG type for each third-party ACD. Most of these ACDs service a single geographic site. Therefore the CRM Connector implementation may need to implement multiple CTIModules, one for each legacy ACD site.

Table 5-2: Cisco CRM Connector Configuration Keys shows the CRM Connector CTIModule configuration keys and valid values. These keys will be referred to in the configuration sections below.

Table 5-2: Cisco CRM Connector Configuration Keys

| Key | Valid Values – Meaning | Meaning / Use |
|---------------|--|--|
| Channel | Four (4) character string Default: CTI1 | The Channel ID. This identifies the channel and is used to associate agent requests with a specific CTI channel. The CTI channel name will show up in the log files on channel events and application commands. |
| Server_A | Hostname or IP address | This is the host name of the CTI Server in a simplex configuration and the host name of the side_A CTI server in a duplex environment. |
| Port_A | Port address, four or five digits | This is the configured CTI Server communication port in a simplex configuration, and the side A CTI Server port in a duplex environment. |
| Server_B | Hostname or IP address | This is only required in a duplex configuration, it is the host name of the side B CTI Server. |
| Port_B | Port address, four or five digits | This is only required in a duplex configuration, it is the port address of the side B CTI Server |
| Peripheral ID | A four digit number. | This is the peripheral ID for the |

| Key | Valid Values – Meaning | Meaning / Use |
|-------------------|---|---|
| | | ACD defined during the installation. For UCCE and UCCH there will be only one Call Manager peripheral, however for UICM there may be more than one peripheral. Each peripheral is treated as a separate site and requires a separate CTIModule configuration. |
| PeripheralType | DEFINITY NORTEL_MERIDIAN NORTEL_SYMPORIUM DMS100 CISCO_CALLMAN | This is the peripheral type for the CTIModule configuration. There can be only one peripheral type per site. UCCE and UCCH implementation will use the CISCO_CALLMAN peripheral type. |
| AssociatedDNsFile | A fully qualified file name, that is one that includes the drive letter, path, file name and file suffix. EX: c:\DNsFiles\Nortel.txt | This text based file serves two purposes: first, it maps the agent primary directory numbers (DN) and their corresponding ACD position ID for Nortel ACDs. This file is required for NORTEL_MERIDIAN and NORTEL_SYMPORIUM. Second, it maps the agent primary directory number and ACD position ID with the Peripheral ID. This is required in multi-site PG configurations, where a PG has more than one PIM. Note that this key name may cause some confusion DNs refers to Directory Numbers (plural), not to IP network DNS information. |
| InternalExtLen | Positive integer, less than or equal to the length of a dial string. Default: 5 | The length of an internal extension. This is used to block screen pops on internal agent-to-agent calls. Most call centers use a dial plan that uses an internal station directory number that is less than the national PSTN dial string. Note: This will not block context screen pops on internal transfers or conferences, but may be used to delay the screen pop until the transfer (or conference) complete |
| DataStore | String, DataStore module name. Default: DataStore | This associates the data store with the CTI module; it is possible to configure multiple CTI modules on a single server as well as multiple data store instances. |
| DefaultReasonCode | A number | This sets the default reason code for implementations where reason codes are used. |

Configuring the CRM Connector for Unified Contact Center

As noted above you will only need to configure a single CTIModule to support the enterprise scale of Unified Contact Center Enterprise and Hosted. This configuration section assumes that you have not already configured a CRM Connector. If you have configured and tested your implementation with the Null CTI connector you will need to edit your config.ini file to replace the NULL CTI connector with the Cisco CRM Connector.

The rest of this section provides step-by-step instructions on implementing the CRM Connector for UCCE or UCCH.

Step 1: Assemble required CTI Server connection information.

In order to configure the Cisco CRM Connector you will need information about your CTI Server configuration.

You will need to know if your system is configured as a simplex or a duplex environment.

1. You will need to know the host name for the CTI Server and the server port. In a duplex environment you will need to know both the Side A and side B host names and ports. In a simplex environment only configure side A.
1. The Unified Contact Center peripheral type is CISCO_CALLMAN. (This is case sensitive.)
2. You will need to know the peripheral ID for the Call Manager Expert Agent PG at your site.
3. If you intend to use a meaningful four character channel name you should plan it in advance, otherwise you may choose the default channel name "CTI1".

Step 2: Backup the config.ini file.

If you are using a text editor, backup the current config.ini file. It is good practice to always edit a copy of a file to guard against accidental changes that affect your system's operation.

Step 3: Open config.ini file for editing.

Use the Administration Tool if you have installed it, or simply navigate to the config.ini file and open it with a text editor.

Step 4: Enable the CRM Connector module in module manager.

This may already be configured, because the default config.ini file includes the module class and module definitions for the CRM Connector. Also the CRM Connector Server implementation chapter included these definitions in the sample config.ini. However we will repeat those steps here.

1. In the module manager create the module class definition for the CRM Connector. This is:
ModuleClass=CiscoCTI,Cisco.AMC_Cisco

2. In the module manager create the module instances, based on the module class:

Module=CTIModule,CiscoCTI

Important Note for Multi-Site Configurations: You must set a unique module name for each module instance. Therefore, if you must create two instances for two legacy ACDs, each must be named uniquely, however each is still assigned the Cisco module class: CiscoCTI.

Note: If you implemented the NULL CTI connector you will need to comment its module instance. It is good practice to comment out the module class definition for unused components, but this is not required.

Warning: If you duplicate instance definitions with the same module name, the **first** defined instance will be implemented. Therefore given the following lines in this order,

Module=CTIModule,CTINullClass

Module=CTIModule,CiscoCTI

Module manager will create the CTINullClass instance. So be sure to comment out any unused module instance definitions. They also consume system resources because they are loaded but unused.

Step 5: Configure the CTIModule connection to CTI Server.

Use the saved settings to enter the CTIModule configuration. See Table 5-2: Cisco CRM Connector Configuration Keys for the configuration key definitions. This table shows the **required** configuration keys.

Example 5-1: UCCE / UCCH CTI Module Section

```
[CTIModule]
Channel=XXXX - enter your four character channel name.
Server_A=<enter your side B hostname>
Port_A=<enter your CTI Server side A port>
Server_B=<enter your side B hostname>
Port_B=<enter your CTI Server side B port>
PeripheralType=CISCO_CALLMAN
PeripheralID=<enter the Call Manager peripheral Id>
```

Step 6: Save the configuration file.

If you are using a text editor save the configuration file, then restart CRM Connector Server to activate the changes. If you are using the Administration Tool, save and activate.

Configuring CRM Connector for UICM

The Unified ICM configuration may be more complex because it requires configurations for third-party ACDs that manage agent ACD sessions. It can also include multiples sites, which require special configuration considerations.

Definition: A multi-site Unified ICM configuration is one where two or more peripherals are served by a single PG type OR one with two or more peripherals served by different PG types.

This section considers a simple, single site configuration but notes changes or additions you will need to make for multi-site configurations. There are two options for multi-site configuration if the ACDs are peripherals on the same PG (PIMS). You may either configure separate instances of CRM Connector for each PIM OR you may configure a single instance of the CRM Connector to support both ACDs. (See the note immediately following for a discussion of the single instances options.)

Important Note for Multi-Site Configuration: In multi-site configurations, where the call center uses two peripherals (PIMS) on the same PG you may optionally configure a single CRM Connector instance to support both ACDs. This adds additional work during configuration: you must create an AssociatedDNsFile that maps **each** ACD extension to its peripheral ID. There are some advantages and several disadvantages to this approach, but it may be useful for some sites.

Key advantage of a single instance configuration for multiple sites on the same PG:

- Reduced configuration within the CRM application. CRM applications must be configured with the Channel ID to associate the agents with their respective channels. Configuring a single instance that supports multiple ACDs allows administrators to assign agents to a common channel configuration. Otherwise you would need to assign the agents individually to the channel configuration.
- Lower maintenance within the CRM application. There is no need to reconfigure an agent to a new channel when moving between ACDs that share a single Connector instance. This may increase agent mobility in large “hot seated” contact centers.

Key disadvantages of a single instance configuration for multiple sites on the same PG:

- Higher maintenance overhead: the AssociatedDNsFile must be updated each time an extension is added.
- Merged reporting and identity. Because a single connector instance can only have one Channel ID, the channel name for both ACDs will be the same. This may make it difficult to report on the ACDs individually within using CRM application reporting tools.
- It may make debugging a little more difficult because you must trace ACDs by their PIMS rather than their Channel ID within the log files.

Step 1: Assemble required CTI Server connection information.

In order to configure the Cisco CRM Connector you will need information about your CTI Server configuration. If you are configuring a multi-site implementation, regardless of whether you are configuring one instance or two, you will need information about both sites.

1. You will need to know if your system is configured as a simplex or a duplex environment.
2. You will need to know the host name for the CTI Server and the server port. In a duplex environment you will need to know both

the side A and side B host names and ports. In a simplex environment, only configure side A.

3. You will need to know the peripheral type. If you are implementing a multi-site that has different ACD types you will need to capture all peripheral types.
4. You will need to know the peripheral ID for the ACD (PIM). If multiple peripherals are implemented you will need to record each peripheral ID.
5. For Nortel Meridian and Symposium sites AND for multiple peripheral sites configured as a single CRM Connector instance you will need a list of agent DNs and their associated ACD DN and the Peripheral ID for the agents and ACDs.
6. You should use meaningful channel names, even if you are only configuring one instance. You will need to assign both a module name AND a channel name. You will need to define a unique module and channel names for each CRM Connector instance.

Step 2: Backup the config.ini file.

If you are using a text editor, backup the current config.ini file. It is good practice to always edit a copy of a file to guard against accidental changes that affect your system's operation.

Step 3: Open config.ini file for editing.

Use the Administration Tool if you have installed it, or simply navigate to the config.ini file and open it with a text editor.

Step 4: Enable the CRM Connector module in module manager.

This may already be configured, because the default config.ini file includes the module class and module definitions for the CRM Connector. Also the CRM Connector Server implementation chapter included these definitions in the sample config.ini. However we will repeat those steps here.

1. In the module manager create the module class definition for the CRM Connector. This is: **ModuleClass=CiscoCTI,Cisco.AMC_Cisco.**
2. In the module manager create this module instance, based on the module manager class: **Module=CTIModule,CiscoCTI.**

Note: If you implemented the NULL CTI connector you will need to comment out its module instance. It is good practice to comment out the module class definition for unused components but this is not required.

Warning: If you have duplicate instance definitions with the same module name configured the **first** defined instance will be implemented. Therefore given the following lines in this order,

Module=CTIModule,CTINullClass
Module=CTIModule,CiscoCTI

Module manager will create the CTINullClass instance. So be sure to comment out any unused module instance definitions. They also consume system resources because they are loaded but unused.

Step 5: Configure the CTIModule connection with the CTI Server.

See Table 5-2: Cisco CRM Connector Configuration Keys for the configuration key definitions. This table shows the **required** configuration keys.

Example 5-2: UICM CTI Module Section

```
[CTIModule]
Channel=XXXX - enter your four character channel name.
Server_A=<enter your side B hostname>
Port_A=<enter your CTI Server side A port>
Server_B=<enter your side B hostname>
Port_B=<enter your CTI Server side B port>
PeripheralType=<peripheral type>
PeripheralID=<enter the Call Manager peripheral Id>
AssociatedDNsFile=c:\Program Files\Cisco\CRM
Connector\MCIS\Connectors\CiscoICM\CiscoLines.txt
```

Step 6: Save the configuration file.

If you are using a text editor save the configuration file. If you are using the Administration Tool, save and activate the new configuration file.

Step 7: Configure the AssociatedDNsFile.

Definition: A DN is a directory number. The agent primary DN is the extension assigned to an agent for direct inbound calls and for performing outbound calls. This may also be referred to as the agent's extension.

The AssociatedDNsFile associates an agent's primary DN with the ACD position ID, this the ID the agent uses to log into the ACD. This file also associates the peripheral IDs for multi-peripheral, single connector instance configurations.

AssociatedDNsFile location.

By default, the AssociatedDNsFile is named "CiscoLines.txt"; it is installed in the CRM Connector directory, the same directory with the config.ini file.

The AssociatedDNsFile format.

The AssociatedDNsFile is divided into two parts: a header section and a body. The file has three columns the first column holds the agent primary DN, the second column holds the agent position ID and the third column the associated peripheral ID. Each column is separated by a dash; there may be white space (spaces or tabs) between the dash and the column entries. Each column **must** have a valid entry. Table 5-4: AssociatedDNsFile below shows a sample AssociatedDNsFile.

The header is two lines. The first line lists each column name separated by white space and a dash. The Table 5-3: AssociatedDNsFile Header Abbreviations below shows column headers abbreviations and their meaning.

Save the AssociatedDNsFile

After you have edited the AssociatedDNsFile to map your agent's DN information save the file. Be sure to save the file in the same location and name you configured in the config.ini file or change the config.ini file for a new location.

Table 5-3: AssociatedDNsFile Header Abbreviations

| Header Abbreviation | Meaning |
|---------------------|-------------------|
| PrimDN | Agent Primary DN |
| PosID | Agent Position ID |
| PeriphID | Peripheral ID |

Table 5-4: AssociatedDNsFile

| PrimDN | - | PosID | - | PeriphID |
|--------|---|-------|---|----------|
| ===== | | | | |
| 1003 | - | 2003 | - | 5007 |
| 1004 | - | 2004 | - | 5007 |
| 9005 | - | 3006 | - | 5003 |
| 1007 | - | 2007 | - | 5007 |

Confirming the CRM Connector Configuration

After you have configured your CRM Connector you will need to test it. Without an application, you will not be able to test CTI command execution, but you can verify that the connector is properly configured, connected to the CTI Server and monitoring the associated peripherals.

Step 1: Start the CRM Connector Server

After changing the config.ini and activating the new configuration file, if you are using the Administration Tool, you will need to restart the CRM Connector Server to apply and activate the changes. You may use the Administration Tool for this or if you are not using the administration tool, use the services control of the Computer Management console to stop and then start the CMService.

Step 2: Check the CTIModule log files.

The CTIModule log file will show the startup sequence for the CRM Connector. **Error! Reference source not found.** below shows an annotated startup sequence for a UICM connection with a Definity peripheral. The last line shows that the CRM Connector is “working” with the Definity.

Example 5-4: Annotated CRM Connector Startup Failure below shows a failed startup: the CRM Connector cannot communicate with the CTI Server because the port configuration is wrong. This also shows that if the connection fails or is lost the CRM Connector will try to establish or re-establish the connection at regular intervals.

Example 5-5: CRM Connector Monitors Agent Extension and Login Logs below shows log snippets that show the monitoring of agent extensions, agent ACD log in sequence and receiving a queued call.

Example 5-3: Annotated CTI Module Startup Log File

| Log File Contents (wrapping lines) | Notes |
|--|--|
| I20070622-110148.696,3476, 0,Initialized Tracing for Module 'CTIModule' | Information – module initializing |
| D20070622-110148.696,3476, 0,Base Initialization for Module 'CTIModule' returning 0x0 | |
| I20070622-110148.696,3476, 0,File Version = 5, 1, 0, 0 | Information – CRM Connector version |
| I20070622-110148.696,3476, 0,CTI Module has been initialized | Information – initialization complete |
| D20070622-110148.790,3476, 0,Base Start for Module 'CTIModule' returning 0x0 | Information – Module started, connecting |
| I20070622-110148.790,3476, 0,CTI Module has been started | |
| D20070622-110148.790,3432, 0,Connect2Cisco: Connecting to Site A (server=amcnt03, port=42027) | Debug – connecting to ICM server, simplex site A info, server_A=amcnt03; port_A=42027 |
| D20070622-110148.806,3432, 0,Connect2Cisco: Currently active is Site 'A' | Debug – side A |
| D20070622-110148.806,3432, 0,OpenRequest: Sending OPEN_REQ (InvokeID=1) | Debug – open request opens the CTI channel to access the Definity server. |
| I20070622-110148.806,3432, 0,EventsMonitor: Connected to Cisco CTI Server, starting event monitoring | Information: CTI Server connection complete; now able to monitor events. |
| D20070622-110148.822,3432, 0,EventsMonitor: Got - OPEN_CONF >>>>> | |
| D20070622-110148.822,3432, 0,InvokeID = 1 | Debug – connecting to a Definity peripheral; this is an UICM configuration using Definity. |
| D20070622-110148.822,3432, 0,ServiceMask = 0x1e | Debug: Information about Definity peripheral configuration. |
| D20070622-110148.822,3432, 0,PeripheralType..... DEFINITY ECS EAS (5) | |
| I20070622-110148.822,3432, 0,OpenConf: Working with DEFINITY (1) | Information: connected and operational with Definity |

Example 5-4: Annotated CRM Connector Startup Failure

| Log File Contents (wrapping lines) | Notes |
|--|---|
| I20070622-110021.708,3072, 0,Initialized Tracing for Module 'CTIModule' | Information – module initializing |
| D20070622-110021.708,3072, 0,Base Initialization for Module 'CTIModule' returning 0x0 | |
| I20070622-110021.724,3072, 0,File Version = 5, 1, 0, 0 | Information – CRM Connector version |
| E20070622-110021.724,3072,-2147467259,GetValues: No value for CTI Server port | ERROR – no value provided for the port. |
| I20070622-110021.724,3072, 0,CTI Module has been initialized | Information – initialization complete |
| D20070622-110021.817,3072, 0,Base Start for Module 'CTIModule' returning 0x0 | Information – Module started, connecting |
| I20070622-110021.817,3072, 0,CTI Module has been started | |
| D20070622-110021.817,2480, 0,Connect2Cisco: Connecting to Site A (server=amcnt03, port=0) | Debug – connecting to ICM server, simplex site A info, server_A=amcnt03; port_A=0 |
| E20070622-110021.817,2480,-2147467259,Connect2Cisco: Cannot connect to server [10049] | ERROR – cannot connect to CTI Server |
| D20070622-110021.817,2480, 0,EventsMonitor: Waiting 15 seconds... | Debug: waiting 15 seconds (to retry) |
| D20070622-110036.822,2480, 0,Connect2Cisco: Connecting to Site A (server=amcnt03, port=0) | Repeating connection attempts...at 30 second intervals |
| E20070622-110036.822,2480,-2147467259,Connect2Cisco: Cannot connect to server [10049] | |
| D20070622-110036.822,2480, 0,EventsMonitor: Waiting 30 seconds... | |
| D20070622-110106.829,2480, 0,Connect2Cisco: Connecting to Site A (server=amcnt03, port=0) | |
| E20070622-110106.829,2480,-2147467259,Connect2Cisco: Cannot connect to server [10049] | |
| D20070622-110106.829,2480, 0,EventsMonitor: Waiting 30 seconds... | |
| D20070622-110136.835,2480, 0,Connect2Cisco: Connecting to Site A (server=amcnt03, port=0) | |
| E20070622-110136.835,2480,-2147467259,Connect2Cisco: Cannot connect to server [10049] | |
| D20070622-110136.835,2480, 0,EventsMonitor: Waiting 30 seconds... | |

Example 5-5: CRM Connector Monitors Agent Extension and Login Logs

| Log File Contents (wrapping lines) | Notes |
|---|--|
| D20070628-155105.819,1128, 0,SnapshotDeviceReq: Sending SNAPSHOT_DEVICE_REQ (InvokeID=2, Ext='24144') | After starting up and connecting with the Definity, the ICM will check for active calls. This log section shows the “snapshot.” |
| D20070628-155105.866,1944, 0,EventsMonitor: Got - SNAPSHOT_DEVICE_CONF >>>>> | |
| D20070628-155105.866,1944, 0,InvokeID = 2 | |
| D20070628-155105.866,1944, 0,NumCalls = 0 | |
| D20070628-155105.866,1944, 0,SnapshotDeviceConf-24144: Updating callsMMap | |
| D20070628-155105.866,1128, 0,SnapshotDeviceReq-24144: End >>> | This sequence shows the assignment and monitoring of an agent DN. The agent is assigning extension 24144. |
| D20070628-155105.866,1128, 0,AddExt2MonExtMap-24144: End >>> | |
| D20070628-155105.866,1128, 0,OpenExtension: Inserting '24144' - '24144' into WorkTopMap | |
| D20070628-155105.866,1128, 0,OpenExtension-24144: End >>> | |
| D20070628-155105.866,1128, 0,TSA-OpenExtension: Exit >>> | |
| D20070628-155105.913, 736, 0,REGISTER-C: Start >>> | “Open Extension” request |
| D20070628-155105.913, 736, 0,REGISTER-C: Registering with EXT=24144 | |
| D20070628-155105.913, 736, 0,QueryAgentState: Sending QUERY_AGENT_STATE_REQ (InvokeID=3, AgentExtension='24144', AgentInstrument='24144') | |
| D20070628-155105.913,1944, 0,EventsMonitor: Got - QUERY_AGENT_STATE_CONF >>>>> | |
| D20070628-155105.913,1944, 0,InvokeID = 3 | |
| D20070628-155105.913,1944, 0,AgentState..... UNKNOWN (9) | Register extension |
| D20070628-155105.913,1944, 0,NumSkillGroups = 0 | |
| D20070628-155105.913,1944, 0,AgentID..... (null) | |
| D20070628-155105.913,1944, 0,AgentExtension..... (null) | |
| D20070628-155105.913,1944, 0,QueryAgentStateConf-24144: Adjusting received agent state: UNKNOWN->LOGOUT | |
| D20070628-155105.913, 736, 0,SnapshotDeviceReq: Sending SNAPSHOT_DEVICE_REQ (InvokeID=4, Ext='24144') | Check current agent state. |
| D20070628-155105.959,1944, 0,EventsMonitor: Got - SNAPSHOT_DEVICE_CONF >>>>> | |
| D20070628-155105.959,1944, 0,InvokeID = 4 | |
| D20070628-155105.959,1944, 0,NumCalls = 0 | |
| D20070628-155105.959,1944, 0,SnapshotDeviceConf-24144: Updating callsMMap | |
| D20070628-155105.959, 736, 0,SnapshotDeviceReq-24144: End >>> | This shows the agent login completed. |
| D20070628-155105.959, 736, 0,GetCiscoCallstate-24144: No calls | |
| D20070628-155105.959, 736, 0,REGISTER-C-24144: Exit - The end | |

6. IMPLEMENTING THE .NET ADAPTER

Purpose

The .Net Adapter is a communication enabler for CRM Connector application adapters. All business application adapters use a .Net adapter configuration to communicate with the CRM Connector Server.

This chapter describes how to configure the .Net Adapter. It explains:

- The role of the .Net Adapter.
- Licensing the .Net Adapter to license all application adapters
- The .Net Adapter type to use with each application adapter
- How to configure .Net Adapter for .Net Remoting.
- How to configure the .Net Adapter for web services, “Soap Adapter.”

.Net Adapter Role

Business application adapters run remotely deployed to business application servers, or agent desktops, or as separate adapter programs. As separate process -- running distributed or “out of process” of the CMService -- they require a means of communicating with the CRM Connector Server.

The .Net Adapter allows distributed business application adapters to communicate with the CRM Connector Server.

You may consider each application adapter to be divided into two parts: a remote standard communication part and an application specific information translation and integration part.

Application adapters form the translation and integration part. They convert contact events and information into business application processes and data using proprietary application APIs. Because the application adapters do not run on the CRM Connector Server they need to be able to communicate with its services.

The .Net Adapter is the standard communication backbone part. It does not provide any application services or maintain state: it only enables communication between two remote systems. It passes messages with contact channel events and information between the CTI Connector Server and the application adapter.

There are two .Net Adapter communication methods: .Net Remoting and ASP.NET web services. The Cisco CRM Connector application adapters use both of these communication enablers.

ASP.NET web services use the SOAP protocol and therefore this .Net Adapter implementation is also referred to as the SOAP Adapter and is

configured with the SoapModule. It is appropriate for web based applications such as PeopleSoft. The SOAP Adapter communicates with the application adapter through web services running on an IIS server. The IIS server acts as an intermediary between the SOAP Adapter and the application adapter. Its application pools execute the services.

.Net Remoting is the second communication enabler. It is more direct and streamlined: there is no intervening web service (IIS). Instead .Net remoting communicates port-to-port between the application adapter and the CRM Connector Server. This is more streamlined and simpler to implement.

.Net remoting is used with application adapters that are run as part of another application. The Salesforce adapter runs within the SalesforceCTL.exe application on the agent's, in the desktop tray.

Licensing .Net Adapters

All application adapters use a .Net Adapter. To simplify licensing, the application adapters use the .Net Adapter license rather than requiring a separate license key for each application's adapter. The .Net Adapter license key is: **AA-DOTNET**

Application Adapter Communication Settings

Each application adapter requires a .Net Adapter sub-component to communicate with the CRM Connector Server. Table 6-1: Application Adapter .Net Adapter Type lists the application adapter and the proper .Net Adapter Type it uses. This information is also included in the Application Adapter Configuration chapters.

Table 6-1: Application Adapter .Net Adapter Type

| Application Adapter | .Net Adapter Type |
|---|-------------------|
| Application Adapter for Oracle PeopleSoft | SOAP Adapter |
| Application Adapter for Microsoft CRM | .Net Remoting |
| Application Adapter for Salesforce.com | .Net Remoting |
| CRM Connector Server Administration Tool | SOAP Adapter |

Configuring .Net Remoting

The .Net Remoting Adapter runs as a CRM Connector Server module. It is configured in the config.ini file and requires the same Module Manager configuration as any other component module: define the module class and then define an instance of the module based on its class. The [RemotingEndpoint] section configures its remote port and other settings.

Module Manager Keys

To enable the .Net Remoting Adapter, add the two keys listed in Table 6-2: .Net Remoting Module Settings to the module manager. Because this is an adapter configuration the settings may be separated from the rest of the core modules.

Table 6-2: .Net Remoting Module Settings

| Key | Valid Values – Meaning | Meaning / Use |
|-------------|---|---|
| ModuleClass | ClassName=RemotingEndPointClass ProgID=AMCNetAdapterRemotingLibrary.RemotingModule | .Net Remote module class definition values. |
| Module | ModuleName=RemotingEndpoint ClassName= RemotingEndPointClass | .Net Remote instance definition. |

Remoting Endpoint Section

The .Net Remoting Adapter configures communication settings for the .Net Adapter. The primary setting is the remoting port with a default value of 5666. All the client adapter systems must configure to connect with the CRM Connector Server on this port. Other configuration settings include event management and a data source as well as the basic global keys.

Table 6-3: Remoting Endpoint Keys

| Key | Valid Values – Meaning | Meaning / Use |
|--------------|--|--|
| RemotingPort | Any valid unused IP socket port above the well known service ports. Default: 5666 | Server remoting port. |
| DataStore | DataStore module name. Default: DataStore | Identifies the data source for the application adapter. With the Cisco CRM Connector this will almost always be DataStore. |

Example 6-1: .NET Remoting Adapter config.ini Section

```
[Module Manager]
.
.
.
### .Net Adapter: Remoting EndPoint
ModuleClass=RemotingEndpointClass,AMCNetAdapterRemotingLibrary.RemotingModule
Module=RemotingEndpoint,RemotingEndPointClass
.
.
.
[RemotingEndpoint]
RemotingPort=5666
DataStore=DataStore
```

Configuring .Net SOAP Adapter Web Services

The .Net SOAP Adapter runs as a CRM Connector Server module. It is configured in the config.ini file. It requires the same Module Manager configuration as any other component module: define the module class and then define an instance of the module class. There is a Remoting Endpoint section that configures the remote port among other settings.

Table 6-4: Soap Adapter Module Settings

| Key | Valid Values – Meaning | Meaning / Use |
|-------------|---|---|
| ModuleClass | ClassName=SoapAdapter4DotNet_ProgrID ProgrID=SoapAdapter4DotNet.SoaAdapterModule | .Net Remote module class definition values. |
| Module | ModuleName=SoapAdapter ClassName=SoapAdapter4DotNet_ProgrID | .Net Remote instance definition. |

Soap Adapter Section

The Soap Adapter section configures the communication connections, event management and data sources for the for .NET web services. It is used by, and must be configured for, the Administration Tool and the PeopleSoft adapter and the Microsoft CRM adapter.

Table 6-5: Soap Adapter Keys

| Key | Valid Values – Meaning | Meaning / Use |
|--------------|--|--|
| EventManager | Name of event manager used with the Soap Adapter. Default: EventManager | Associates an event manager with the Soap Adapter. In large implementations, more than one event manager may be configured to support dedicated communications requirements. |
| DataStore | DataStore used with the .NET adapter. Default: DataStore | Associates the data store used by the application adapter; this should be the same data stored used by the connector. |
| EventRaiser | AMCDotNetEventAdapterRaiser.MSMQ-EventRaiser | This associates a .NET event web service. |

Example 6-2: .NET SOAP Adapter config.ini Section

```
[Module Manager]
.
### .Net Adapter: SOAP Adapter
ModuleClass=SoapAdapter4DotNet_ProgrID,SoapAdapter4DotNet.SoaAdapterModule
Module=SaopAdapter,SoapAdapter4DotNet_ProgrID
.
[SoapAdapter]
EventManager=EventManager
DataStore=DataStore
EventRaiser=AMCDotNetEventAdapterRaiser.MSMQEventRaiser
```

7. IMPLEMENTING THE SALESFORCE.COM ADAPTER

Purpose

This Chapter describes the procedures to implement the Salesforce.com application adapter. This adapter integrates with the Salesforce.com hosted CRM application. The adapter is installed on the agent desktop PC and connects to the CRM Connector Server through .NET Remoting.

This chapter covers:

- Pre-installation Requirements
- The Salesforce.com distributed architecture
- Installing the Salesforce.com Application Adapter
- Configuring the Salesforce.com Application Call Center Edition

Overview: Implementation Process Steps.

Before performing any installation or implementation work you should read this entire chapter. This section lists the implementation process steps; later sections provide step-by-step implementation instructions.

- Implement both the Cisco CRM Connector Server and the Cisco CRM Connector for UICM, UCCE and UCCH.
- Create two configurations to one support the Null CTI Server and the other for Cisco CRM Connector for UICM, UCCE and UCCH.
- Configure the .Net Adapter for .NET Remoting on the CRM Connector Server.
- Install .Net Framework V2.0 on the desktop PC for all call center agents who will use the application adapter.
- Install the Cisco Application Adapter for Salesforce.com on the agents' desktop PCs.
- Install Microsoft Internet Explorer 6.0 or higher on the agents' desktop PCs.
- Install and Configure the Salesforce.com definition file.

Additional steps you may wish to take that are not covered in this implementation guide.

- Modify your standard agent desktop image to include the Microsoft .Net Framework and Salesforce.com adapter file.
- Use a Windows application tool to push updates and patches to the agent desktop.

This implementation varies from the typical implementation. Because the application files are maintained at the agent desktop, the test / development environment should include a reference administrator's desktop that includes the Salesforce.com application adapter. This desktop can be used to administer and configure the Salesforce.com Call Center edition.

Pre-Installation Requirements

You will need a subscription to Salesforce.com Call Center Edition. Call Center Edition is a new component of the Professional, Enterprise and Unlimited Editions starting with Winter 2007.

Before installing the Cisco Application Adapter for Salesforce.com you must perform these steps.

Step 1: Implement Cisco CRM Connect Server.

CRM Connector Server must be installed, configured and operational before you implement any additional CRM Connector components.

Step 2: Implement the Cisco CRM Connector for Unified ICM and Unified Contact Center Enterprise and Hosted and the Null CTI Connector configuration for initial testing.

You should have configurations that support both the live Cisco CRM Connector and the Null CTI connector. This will allow testing the application adapter independently of other connection and CTI considerations before testing with live CTI.

Once the application adapter installation is confirmed using the Null CTI Connector, use the Cisco CRM Connector for live phone call tests.

You may create this configuration using separate config.ini files, by commenting out the Cisco CRM Connector while testing the Null connector, or with separate CTI Modules, one for the Null CTI Connector and another for the live Cisco CRM Connector.

Step 3: Install Microsoft .Net Framework V2.0 on each agent's desktop.

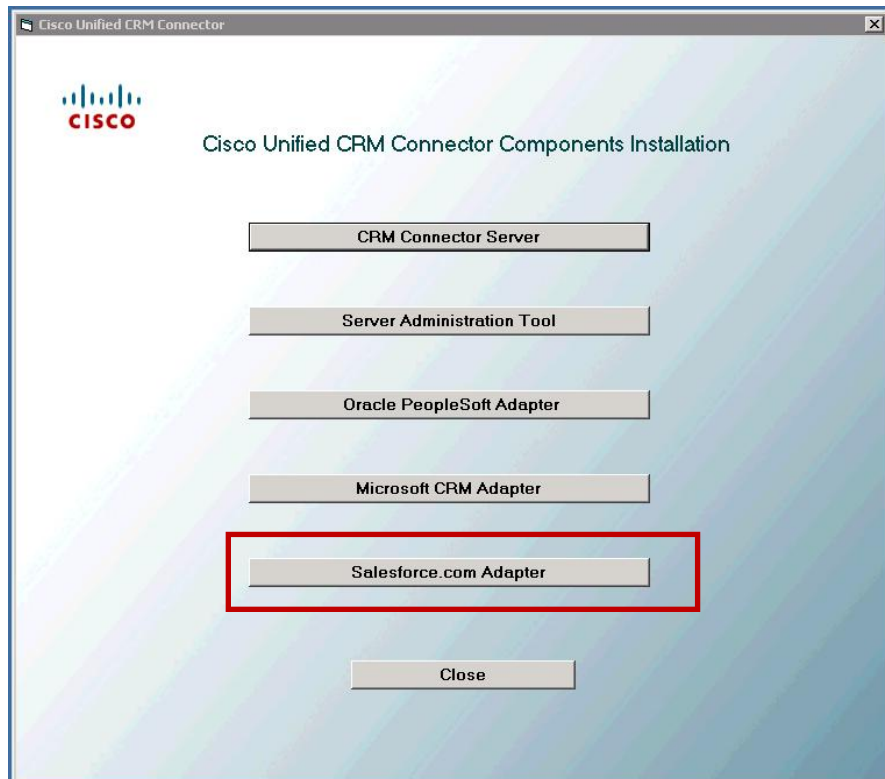
The Salesforce.com adapter must be installed on each agent's desktop. This is part of the Salesforce.com Call Center Edition architecture. The adapter connects with CRM Connector Server using .NET remoting.

Installing Salesforce.com Software

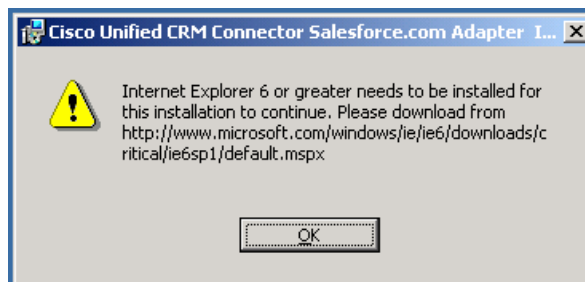
The Salesforce.com software installation on the agent desktop is very straightforward.

There are no installation options. The wizard installs the application adapter software on the agent's C: drive. Table 7-1: Salesforce Application Adapter Directory Structure shows the default directory structure and installed files.

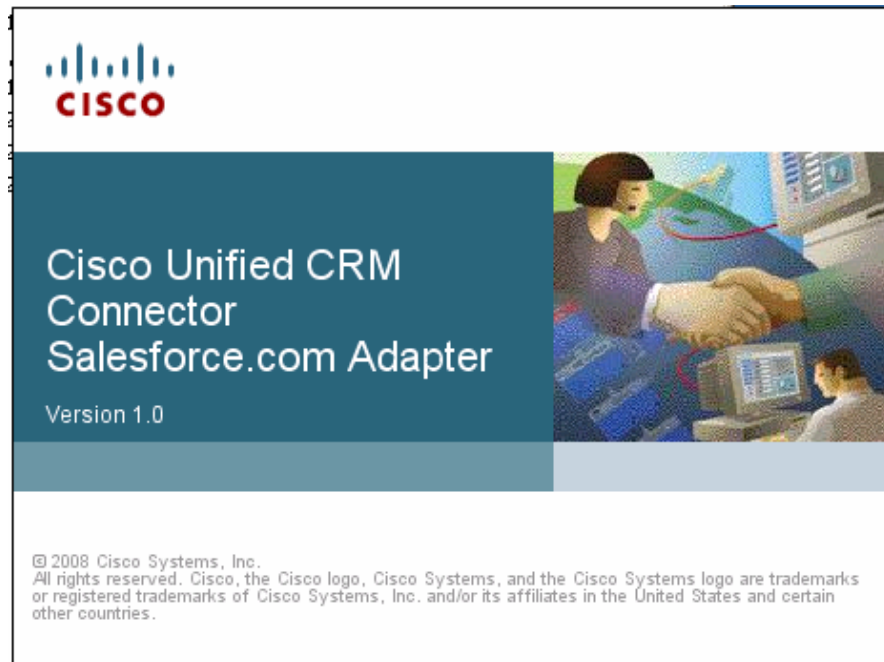
Step 1: Start the installation and select the Salesforce.com component.



- The Cisco Application Adapter for Salesforce.com requires Internet Explorer 6.0 or higher. If IE is not installed on the target machine, you will be warned and the installation will abort.

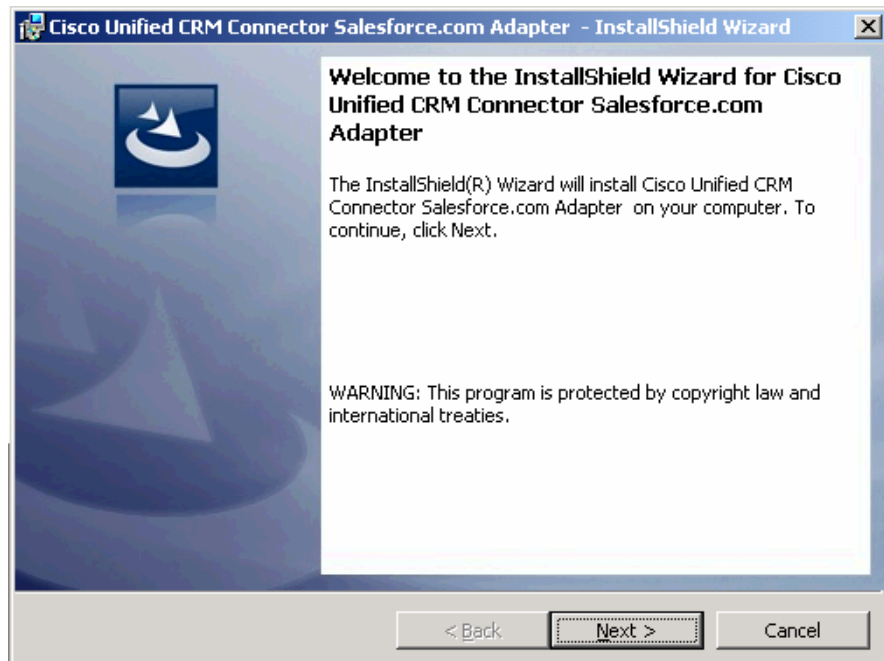


- If Microsoft .Net Framework V2.0 is not installed on the agent desktop PC InstallShield wizard will install it. Otherwise you will be presented five informative wizard dialogs that require a response to continue:

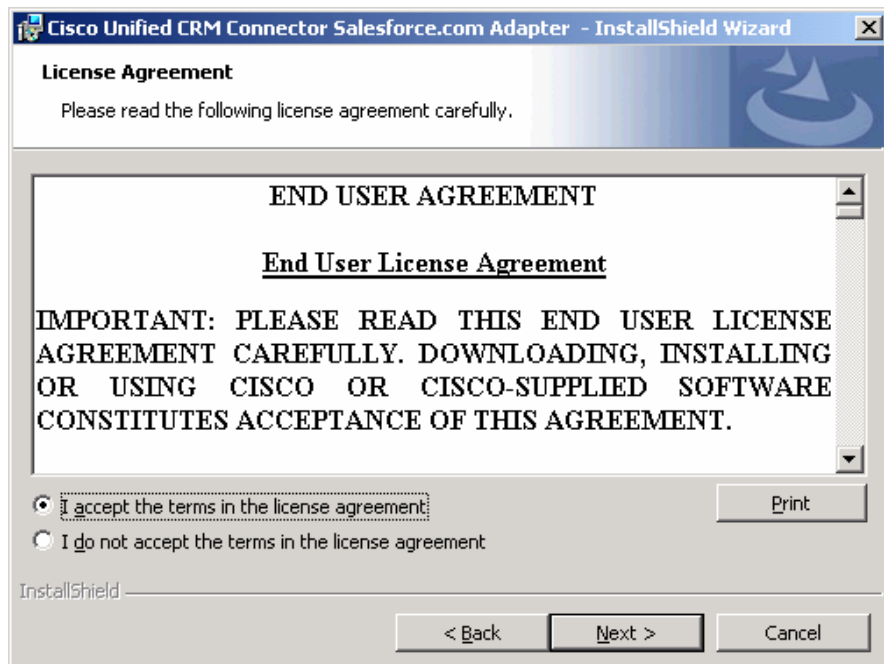


Step 2: Begin the install and accept the End User License Agreement.

- You are greeted with the installation splash screen and then the InstallShield Wizard dialog; press Next to start the installation.

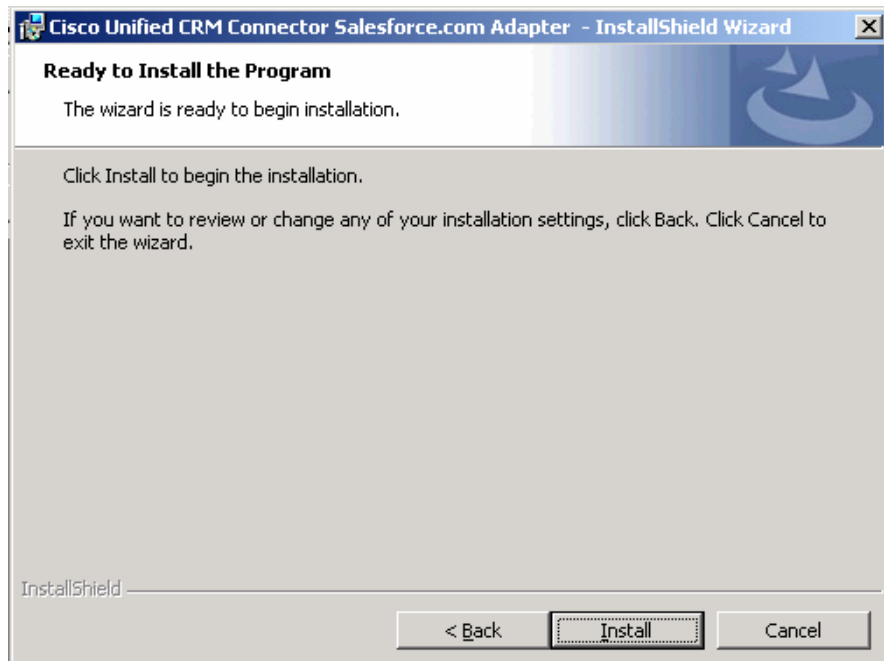


- You are prompted to accept the End User License Agreement (EULA). Read the agreement and then press the radio button to accept and press Next to continue.

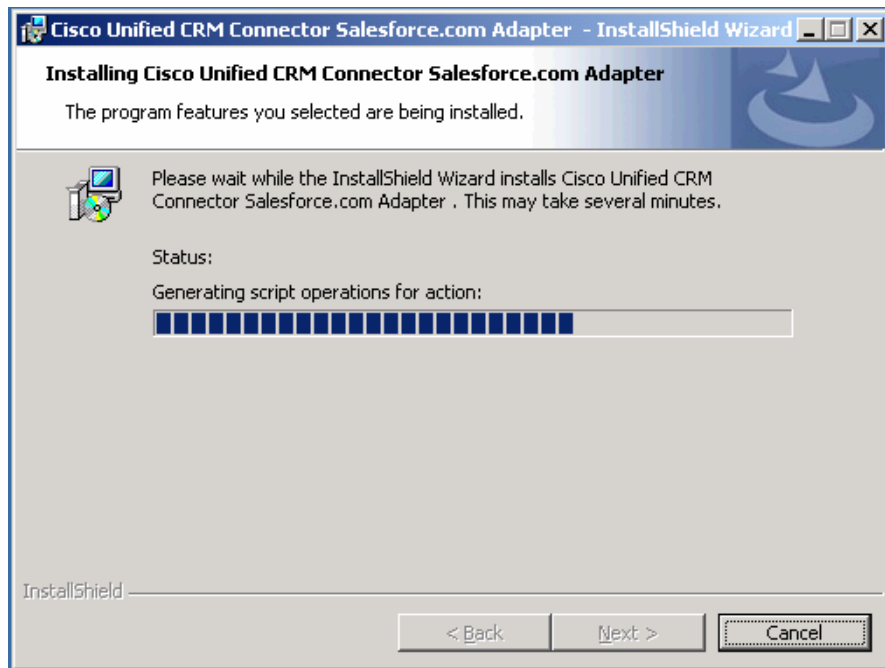


Step 3: Start the install.

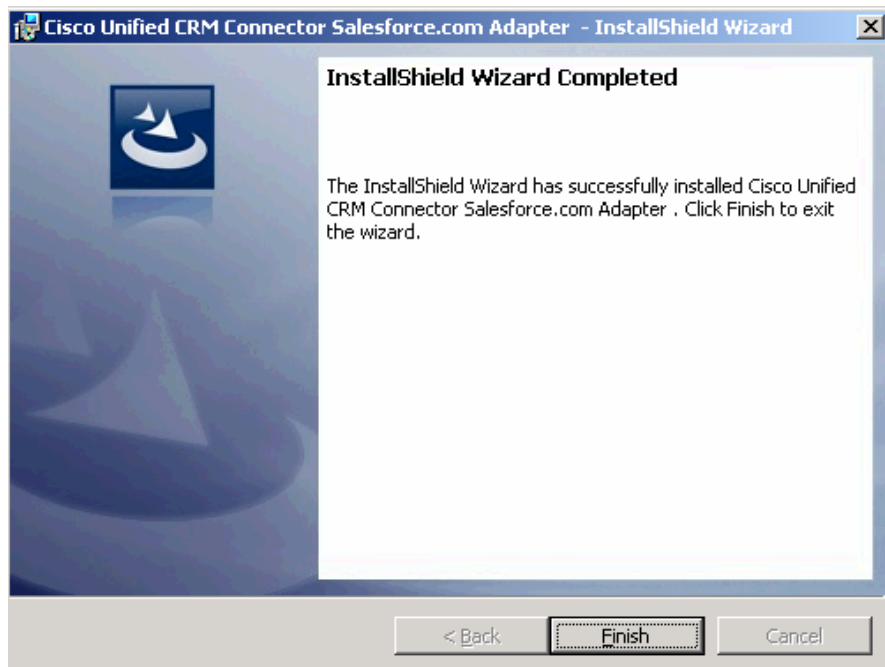
- You are next prompted to start the installation. The software is automatically installed on the agent PC system drive. Press **Install** to start the installation.



- During the installation the install wizard dialog shows the installation progress bar.



- When the installation is complete you are informed and prompted to press Finish to complete the install.



Note: you may wish to develop a distribution package that pushes the Salesforce.com application adapter and future patches to the agent desktop. That is beyond the scope of this documentation.

Table 7-1: Salesforce Application Adapter Directory Structure

| Sub-Directory | Component | Use |
|---|--|---|
| <Windows SystemDrive>\Program Files\Cisco\ | | <p>This is the parent drive location; all agent desktop application adapters will be installed under this directory hierarchy</p> <p>Note: To identify the Windows system drive open a command prompt</p> <p>Start->Run->cmd.</p> <p>Use the command “set system” this will show any environment variable that contains “system.” It will show a value “SystemDrive=<drive letter...>”</p> |
| C:\Program Files\Cisco\CRM Connector\Salesforce.com Adapter | | <p>This is the Salesforce.com application adapter sub-directory. All application files and configuration files in this directory. Some log files are also recorded to this directory.</p> |
| | Cisco_Salesforce_CallCenter.xml | <p>Cisco Salesforce.com application adapter configuration definition file. This file needs to be imported into your Salesforce.com call center configuration once to set the default parameters.</p> <p>This file is not accessed from the agent desktop; instead the agents download their configuration through their standard Salesforce.com browser connection.</p> |
| | SalesForceCTI.exe SF_MSApril.dll | <p>Salesforce application adapter executable and support files distributed to the local desktop. This salesforce.com communication software runs in the agent’s PC system tray.</p> |
| | amcctiadaper.dll | <p>Cisco Salesforce.com channel integration adapter.</p> |
| | AMCCommonInterfaces.dll AMCOMMONINTERFACESLib.dll AMCMultiChannelInterface.dll AMCMULTICHANNELINTERFACESLIB.dll AMCSystemTools.dll CONTACTOBJECTSLib.dll StandardObjects.dll STANDARDOBJECTSLIB.dll | <p>Cisco Salesforce.com general support utility services.</p> |
| | AMCDotNetAdapterLibrary.dll AMCDotNetAdapterRemotingLibrary.dll AMCDotNetAPI.dll | <p>Cisco .NET remoting communications support utility services.</p> |
| | Atl71.dll msvcp71.dll msvcr71.dll | <p>Software library development tool distributable from Microsoft to support Cisco application files.</p> |

| Sub-Directory | Component | Use |
|---|-----------------------|---|
| | Browser_connector.log | This is the salesforce.com log file that tracks channel communications between the application adapter and the user's browser session. |
| | Cti_connector.log | This is the salesForce.com log file that tracks channel communications between the Salesforce.com application adapter and the Salesforce.com hosted services. |
| C:\Program Files\Cisco\CRM Connector\Salesforce.com Adapter \Logs | | This is the Cisco Salesforce.com Application Adapter logs directory. This location is configured within Salesforce.com administration. |
| | SalesForceAdapter.log | This is the Cisco log file for the Salesforce.com Application Adapter |

Configuring the Salesforce.com Adapter

Quick Summary

There are no local configurations maintained on the agent desktop. Once the software is deployed to the agent desktop you must configure the .Net Adapter for .Net Remoting. The rest of the configuration is implemented in the Salesforce.com Administration Setup utilities, part of the Salesforce.com hosted applications.

You may install the Salesforce.com adapter on the CRM Connector Server machine, but this is not required. You will need to install it on an administrator's desktop. This is considered a deployment approach and is not documented here.

Configure and License the .Net Adapter for .Net Remoting

Step 1. Configure the .Net Adapter for .Net Remoting communication interface in the config.ini.

See [Chapter 6: Implementing the .NET Adapter](#) for instructions on implementing the .Net Adapter for .Net Remoting.

Step 2. Apply license for the .Net Adapter.

You may defer this step until after the installation is complete. There is a thirty-day post installation implementation period before licensing is enforced. See the Administration Tool Chapter 4 for licensing procedures.

Import the Call Center Configuration

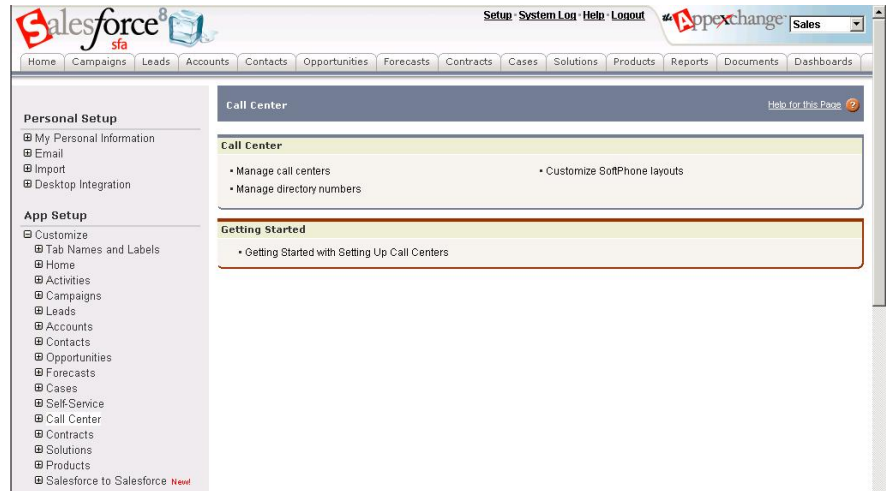
Step 3. Log into Salesforce.com as the system administrator

Use a Microsoft Internet Explorer browser to navigate to the Salesforce.com web site. Log in with the system administrator account.

Step 4. From the Salesforce.com Home Page navigate to the administration page

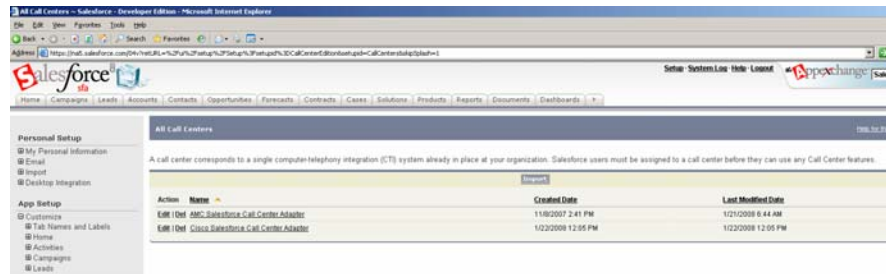
Use the setup link on the Home page to navigate to the Salesforce.com administration page.

Step 5. Select Call Center under the App Setup->Customize option from the left hand navigation bar.



Navigate to the call center configuration page. Select the option “Call Centers” from the left side navigation bar. Then select “Manage Call Centers” from the Call Center page to configure the Salesforce.com adapter.

Step 6. Import the call center configuration definition file.



The “All Call Centers” page allows you to manage your call center configurations. Use the edit links to the left of the call center summary line to edit or delete existing call center configurations. Use the “Import” link to import new call center definitions.

Note: This screen shot shows existing call center configurations. When you first log into Salesforce.com there will not be any pre-configured call centers. This documentation continues with instructions on the importation of a new call center configuration.

Step 7. Edit the call center definition file with your CRM Contact Center configurations before importing.

The Cisco Application Adapter for Salesforce.com installs a generic call center configuration file. This is an XML file named

Cisco_Salesforce_CallCenter.xml. The contents of the generic install file are shown in Example 7-1: Generic Call Center Definition XML File.

Note: You do not need to edit the generic call center definition file. You can always change these parameters in the Salesforce.com call center configuration administration. However, setting the defaults for your call center will reduce edits to the call center configuration after the file is imported.

Edit XML files using any text editor, or use an XML editor; freeware versions are available on the web.

When editing this file for your call center, you should edit the following entries in the “MCISInfo” section. These are the lines following this XML entry:

- <section sortOrder="1" name="MCISInfo" label="AMC MCIS Server Information">

1. Change the server name on the “Server” item line. The default is AMCXPGMZ. Enter the host name (or IP address) of the CRM Connector Server.
<item sortOrder="0" name="Server" label="MCIS Host">AMCXPGMZ</item>
2. The RemotePort refers to the .NET Remoting port from the config.ini file. The Event Port is the used to communicate back to Salesforce.com. Only change these if you have changed the ports to meet local network requirements.
3. Set the “Channel ID” to match the CRM Connector Channel ID. The default is CTI1 but this MUST match the Channel name in the CTIModule.
<item sortOrder="3" name="ChannelID" label="ChannelID">CTI1</item>
4. Enter your call center’s default queue information.
<item sortOrder="4" name="Queue" label="Queue">62</item>
5. You may also wish to edit the dialing options section to match your local dial plan. This sets:
 - the outbound dial prefix, used to get an outside line;
 - the long distance country code prefix (“1” in the United States),
 - and the international dialing prefix (“01” in the United States).
6. You may also set the display name to match your call center in the first section “General Information.”
7. After completing your edits save the new call center definition with a new name, preserving the default version.

Example 7-1: Generic Call Center Definition XML File

```
<?xml version="1.0" encoding="UTF-8" ?>
- <callCenter>
- <section sortOrder="0" name="reqGeneralInfo" label="General Information">
  <item sortOrder="0" name="reqInternalName" label="Internal Name">AMCCTIAdapter</item>
  <item sortOrder="1" name="reqDisplayName" label="Display Name">AMC Call CTI Center Adapter</item>
  <item sortOrder="2" name="reqDescription" label="Description">AMC Call Center CTI Adapter</item>
  <item sortOrder="3" name="reqProgId" label="CTI Connector ProgId">AMCCTIAdapter.AMCCTIAdapter.1</item>
</section>
```



```

- <section sortOrder="1" name="MCISInfo" label="AMC MCIS Server Information">
  <item sortOrder="0" name="Server" label="MCIS Host">AMCXPGMZ</item>
  <item sortOrder="1" name="RemotePort" label="Remote Port">5666</item>
  <item sortOrder="2" name="EventPort" label="Event Port">5558</item>
  <item sortOrder="3" name="ChannelID" label="ChannelID">CTI1</item>
  <item sortOrder="4" name="Queue" label="Queue">62</item>
</section>
- <section sortOrder="2" name="reqDialingOptions" label="Dialing Options">
  <item sortOrder="0" name="reqOutsidePrefix" label="Outside Prefix">9</item>
  <item sortOrder="1" name="reqLongDistPrefix" label="Long Distance Prefix">1</item>
  <item sortOrder="2" name="reqInternationalPrefix" label="International Prefix">01</item>
</section>
</callCenter>

```

Step 8. Import the Call Center definition file.

1. Select the “Import” link on the All Call Centers administration page.
2. Use the browse option to navigate to the directory with the Cisco_Salesforce_CallCenter.XML and select the file to import it.
3. After selecting the file, press “Import” to import the new call center configuration.
4. This will open the “Call Center Detail” page where you can modify the call center configuration.

Edit your Call Center Configuration

Note: You will only need to perform the edits for steps 10, 11 and 14 if you did not edit the call center configuration definition file.

The rest of these configuration steps should be reviewed and may need to be set.

Salesforce.com has very good on-line documentation explaining most of the configurations and their use. These instructions are provided here for your convenience.

Step 9. Edit the Adapter Configuration Information.

Call Center: Cisco Salesforce Call Center Adapter

Call Center Detail

General Information

| | |
|----------------------|--------------------------------------|
| Internal Name | CiscoSalesForceCallCenter |
| Display Name | Cisco Salesforce Call Center Adapter |
| Description | Cisco Salesforce Call Center Adapter |
| CTI Connector ProgID | AMCCTAdapter.AMCCTAdapter.1 |

Cisco CRM Connector Information

| | |
|----------------------|-----------|
| CRM Connector Server | AMCW23009 |
| Remote Port | 5886 |
| Event Port | 5558 |
| ChannelID | CTI1 |
| Queue | 62 |

Adapter Trace Information

| | |
|-------------|--|
| Using Log | True |
| Trace Path | C:\Program Files\Cisco\CRM Connector\Salesforce.com Adapter\Log1 |
| Trace Level | 4 |

Setting for Reason Code

| | |
|--------------------------------|-------|
| Enabling Not Ready Reason Code | False |
| Enabling Logout Reason Code | False |
| Enabling Wrapup Reason Code | False |

The internal name and the CTI ProgID fulfill the role of the module class definition and module instance definition in the ModuleManager. For each call center configuration you may need to set the internal name, display name and description; do not change the CTI Connector ProgID.

Step 10. Edit Server Connection Information

Call Center: Cisco Salesforce Call Center Adapter

Call Center Detail

General Information

| | |
|----------------------|--------------------------------------|
| Internal Name | CiscoSalesForceCallCenter |
| Display Name | Cisco Salesforce Call Center Adapter |
| Description | Cisco Salesforce Call Center Adapter |
| CTI Connector ProgID | AMCCTAdapter.AMCCTAdapter.1 |

Cisco CRM Connector Information

| | |
|----------------------|-----------|
| CRM Connector Server | AMCW23009 |
| Remote Port | 5886 |
| Event Port | 5558 |
| ChannelID | CTI1 |
| Queue | 62 |

Adapter Trace Information

| | |
|-------------|--|
| Using Log | True |
| Trace Path | C:\Program Files\Cisco\CRM Connector\Salesforce.com Adapter\Log1 |
| Trace Level | 4 |

Setting for Reason Code

| | |
|--------------------------------|-------|
| Enabling Not Ready Reason Code | False |
| Enabling Logout Reason Code | False |
| Enabling Wrapup Reason Code | False |

Edit the server information to match the CRM Connector Server information. Note that these changes affect the agent's machine.

- The CRM Connector Server is the host name or IP address of the CRM Connector Server.
- The Remote Port is the .Net Adapter .Net Remoting port setting.
- The Event Port is used to communicate with Salesforce.com; if a firewall is active on the agent machine this port must be opened.

- The Channel ID is the CTIModule “Channel” name. This must match the agent’s assigned CRM Connector configuration.
- The Queue is the either the default queue for this contact center configuration or a “phantom” queue used by the CRM Connector to log into the ACD.

IMPORTANT WARNING: You must specify a default queue in the Salesforce.com adapter settings. You **must assign** a queue to each Salesforce.com call center agent, even if you do not use queues (or skills) in UCC or the ICM integrated ACD. You may assign a “phantom” queue value, such as 1, 10 or 9999. Agents will not be able to log in without this queue assignment.

Step 11. Enter the log tracing levels and log file locations.

The screenshot shows the Salesforce Call Center Adapter configuration page. The left sidebar contains navigation links for Personal Setup, App Setup, and Customization. The main content area is titled 'Call Center: Cisco Salesforce Call Center Adapter'. Under 'Call Center Detail', there are sections for General Information, Cisco CRM Connector Information, and Adapter Trace Information. The Adapter Trace Information section is highlighted with a red box and contains the following settings:

| Adapter Trace Information | |
|--------------------------------|---|
| Using Log | True |
| Trace Path | C:\Program Files\Cisco\CRM Connector\Salesforce.com Adapter\Log |
| Trace Level | 4 |
| Enabling Not Ready Reason Code | False |
| Enabling Logout Reason Code | False |
| Enabling Wrapup Reason Code | False |

In the “AMC Trace Information Section” enable tracing, set the trace file locations and the tracing level.

- Using Log: Set this “True” to enable tracing.
- Trace Path: Enter the directory on the agent’s desktop PC where the log files will be stored. Note that the log files are stored on the agent’s PC and are local to each agent’s Salesforce.com sessions.
- Set the Trace Level: The Salesforce.com application adapter supports an enhanced debug trace level, four (4).

Step 12. Enable and define reason codes.

| | |
|---|---|
| Call Center | |
| Cisco Salesforce Call Center Adapter | |
| All Call Centers > Cisco Salesforce Call Center Adapter | |
| Call Center Detail Edit Delete Clone | |
| General Information | |
| Internal Name | CiscoSalesForceCallCenter |
| Display Name | Cisco Salesforce Call Center Adapter |
| Description | Cisco Salesforce Call Center Adapter |
| CTI Connector ProgId | AMCCTIAdapter.AMCCTIAdapter.1 |
| Cisco CRM Connector Information | |
| CRM Connector Server | AMCW23S09 |
| Remote Port | 5666 |
| Event Port | 5558 |
| ChannelID | CTI1 |
| Queue | 62 |
| Adapter Trace Information | |
| Using Log | True |
| Trace Path | C:\Program Files\Cisco\CRM Connector\Salesforce.com Adapter\Logs\ |
| Trace Level | 4 |
| Setting for Reason Code | |
| Enabling Not Ready Reason Code | False |
| Enabling Logout Reason Code | False |
| Enabling Wrapup Reason Code | False |
| List of Reason Codes | |
| Numbers of Reason Codes | 2 |
| 1 | Lunch |
| 2 | Personal |
| Dialing Options | |
| Outside Prefix | 9 |
| Long Distance Prefix | 1 |
| International Prefix | 01 |

Setting for Reason Codes

Reason codes are used by some contact centers to report the reason why an agent went into an idle state: for example, to take lunch or a break. These codes are configured on the switch and reported by the switch. There are three reason codes types that may be enabled or disabled in this section:

- Not Ready Reason: This requires a reason whenever an agent sets themselves “Not Ready.” For example before lunch or taking a break.
- Logout Reason Code: This requires a reason code whenever an agent logs out of the ACD.
- Entering Wrapup Reason Code: This records a reason code whenever the agent enters a wrapup state. This is used to capture call outcomes for switch reporting and analysis.

The “entering wrapup reason code” is rarely configured as most CRM applications capture this information and provide more detailed reporting on the activities and other aspects of the customer interaction. If this is enabled, consider setting the default reason code parameter in the CTIModule.

List of Reason Codes

If Reason Codes are enabled you will need to enter supported reason codes and their description within the “List of Reason Codes” section. The reason code list consists of a reason code number and a description. The number matches the reason code configured on the switch. The reason code description is provided to the agents so they do not need to memorize the meaning of the numbers.

Step 13. Set the Dialing Options

| Call Center Cisco Salesforce Call Center Adapter | |
|---|---|
| All Call Centers » Cisco Salesforce Call Center Adapter | |
| Call Center Detail Edit Delete Clone | |
| General Information | |
| Internal Name | CiscoSalesForceCallCenter |
| Display Name | Cisco Salesforce Call Center Adapter |
| Description | Cisco Salesforce Call Center Adapter |
| CTI Connector Progid | AMCCTIAdapter.AMCCTIAdapter.1 |
| Cisco CRM Connector Information | |
| CRM Connector Server | AMCW23S09 |
| Remote Port | 5666 |
| Event Port | 5558 |
| ChannelID | CTI1 |
| Queue | 62 |
| Adapter Trace Information | |
| Using Log | True |
| Trace Path | C:\Program Files\Cisco\CRM Connector\Salesforce.com Adapter\Logs\ |
| Trace Level | 4 |
| Setting for Reason Code | |
| Enabling Not Ready Reason Code | False |
| Enabling Logout Reason Code | False |
| Enabling Wrapup Reason Code | False |
| List of Reason Codes | |
| Numbers of Reason Codes | 2 |
| 1 | Lunch |
| 2 | Personal |
| Dialing Options | |
| Outside Prefix | 9 |
| Long Distance Prefix | 1 |
| International Prefix | 01 |

The dialing options set outbound dial prefixes to match the call center’s local dial plan. These options may work with the “Define Prefix” settings listed below to automatically set the dial prefix for local, long distance and international calls.

- **Outside Prefix:** The digits agents must dial to get an outside (PSTN) dial tone.
- **Long Distance Prefix:** The digits required to complete a long distance dial. In the United States this is the country code.
- **International Prefix:** The digits required to complete an international dial. In the United States this is “01”

| Define Prefix | |
|--------------------------------|-------|
| Enabling Prefix settings | False |
| Length of Outside Prefix | 7 |
| Length of Long Distance Prefix | 10 |
| Length of International Prefix | 12 |

For outbound dials, Salesforce.com can distinguish the call type based on the length of the dial string and affix the appropriate prefix. Use the “Define Prefix” settings to set the length for local (outside) calls, long distance calls and international calls. If the dial string is less than the “Outside Prefix” length it is considered an internal (agent-to-agent) call.

These settings are:

- **Enabling Prefix settings:** This activates prefix determination. The choices are true and false. True enables outbound prefix assignment. False disables it. False is the default.
- **Length of Outside Prefix:** This is the length of an outbound local call dial string. The default is 7, which is standard in the United States.
- **Length of Long Distance Prefix:** This is the length of an outbound long distance call dial string. The default is 10, which is standard in the United States.
- **Length of International Prefix:** This is the length of an outbound international call dial string. The default is 12, which is standard in the United States.

Create, Configure and Assign Agents for the Call Center

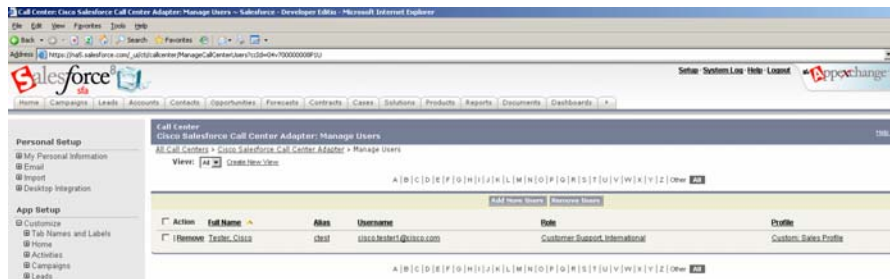
Step 14. Navigate to the Agent Management page

The Call Center Users information at the bottom of the call center page lists the number of users assigned to the call center and provides a link to manage call center users. Use the link to navigate to the user administration page.

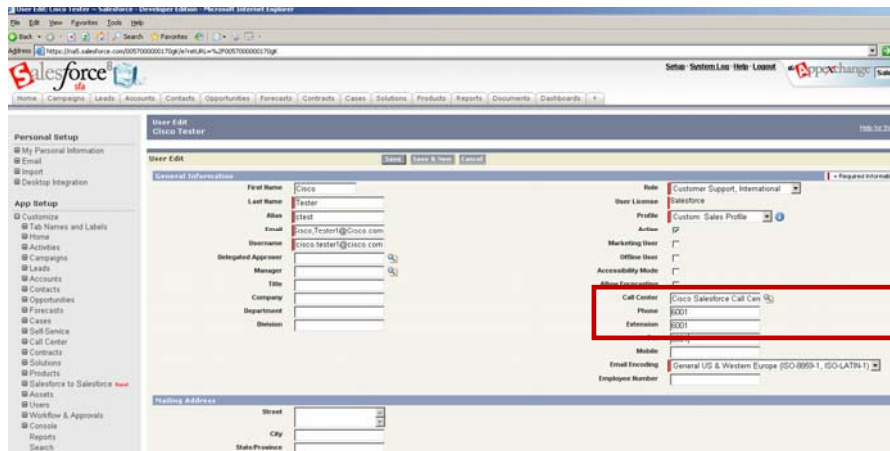
Step 15. Navigate to the Agent Management page

The manage users page provides links to create new users, delete or change the configuration for existing users.

Selecting the agent’s name will navigate to the agent configuration page.



Step 16. Edit a user's call center configuration



On the agent configuration page you may set the agent's roles and designate a profile for the agent.

Assign the agent to a call center and assign the agent phone number and extension. Note that the ACD configuration is set by the agents in the Salesforce.com softphone when they log into the ACD, so you do not need to include the extension. This supports "hot seating," sometimes called "free seating" or "hotelling."

8. IMPLEMENTING THE ORACLE PEOPLESOFT ADAPTER

Purpose

This Chapter describes the procedures to implement the CRM Application Adapter for Oracle PeopleSoft. This adapter provides direct, server-level integration with PeopleSoft's PeopleTools Multi-Channel Framework.

This chapter covers:

- Pre-installation Requirements.
- Installing the CRM Application Adapter Oracle PeopleSoft
- Application Adapter Configuration
- PeopleSoft PeopleTools Configuration

Overview: Implementation Process Steps.

Before performing any installation or implementation work you should read this entire chapter. This section lists the implementation process steps; later sections provide step-by-step implementation instructions.

- Implement both the Cisco CRM Connector Server and the Cisco CRM Connector for UICM, UCCE and UCCH.
- Create two configurations: one support the Null CTI Server and the other for Cisco CRM Connector for UICM, UCCE and UCCH.
- Configure the .Net Adapter for Soap web services (.NET Soap Adapter.).
- Configure PeopleTools REN Server and Multi-Channel Framework
- Install the Cisco Application Adapter for Oracle PeopleSoft on the CRM Connector Server
- Configure the PeopleSoft Adapter

This implementation varies from the typical implementation. The PeopleSoft APIs, "PSMCAPI" are Java APIs that need to run within a Java Virtual Machine. The Oracle PeopleSoft application adapter includes a service that launches the PSMCAPI Java Virtual Machine. Also, because of the PeopleSoft architecture, the PeopleSoft application adapter communicates through the .Net Soap Adapter web services.

Pre-Installation Requirements

- The PeopleSoft application adapter requires the Java Runtime Environment (JRE). Check with Oracle to determine which version of the JRE your PeopleTools version requires.
- The PeopleSoft application adapter requires PeopleTools 8.45 or later. Cisco recommends a minimum version of PeopleTools 8.47.
- The PeopleSoft application adapter requires a Windows operating environment. Even though the adapter is Java based, it depends upon a windows service to launch and control the Java virtual machine.
- The PeopleSoft application adapter requires configuring the REN server. The REN server may co-reside with the CRM Application Adapter for Oracle PeopleSoft. If REN server runs on a remote machine, it does not need to use the Windows operating system; it can use Linux or other Oracle supported operating systems.
- The PeopleSoft application adapter uses the .NET Adapter for Soap web services. This must be implemented and licensed.

Pre-Installation CRM Connector Steps

Before installing the Cisco Application Adapter for Oracle PeopleSoft you must perform these steps.

Step 1: Implement Cisco CRM Connector Server.

CRM Connector Server must be installed, configured and operational before you implement any additional CRM Connector components.

Step 2: Implement the Cisco CRM Connector for UICM, UCCE and UCCH and the Null CTI Connector configuration for initial testing.

You should have configurations that support both the live Cisco CRM Connector and the Null CTI connector. This will allow testing the application adapter independently of other connection and CTI considerations before testing with live CTI.

Once the application adapter installation is confirmed using the Null CTI Connector, use the Cisco CRM Connector for live phone call tests.

You may create this configuration using separate config.ini files, by commenting out the Cisco CRM Connector while testing the Null connector, or with separate CTIModules, one for the Null CTI Connector and another for the live Cisco CRM Connector.

Step 3: Install Microsoft .Net Framework V2.0 on the application adapter server.

In most implementations the PeopleSoft adapter runs on the CRM Connector Server; this should already have .Net Framework version 2.0 installed.

Pre-Installation Oracle PeopleSoft Steps

You will need to configure the Oracle PeopleSoft Multi-Channel Framework for the Cisco CRM Connector. This is the responsibility of an Oracle System Administrator. The configuration is documented in Oracle PeopleBooks.

As a convenience, this documentation provides step-by-step in assistance guidance in the next section. However you should consult the Oracle documentation and your PeopleSoft System Administrator to verify proper configurations.

Before You Begin

Before installing the software you will need:

- PeopleSoft user agent and REN server login user accounts.
- The host name or IP address of the server running the REN server.
- The URL for the PeopleSoft application environment.

Configuring Oracle PeopleSoft Multi-Channel Framework

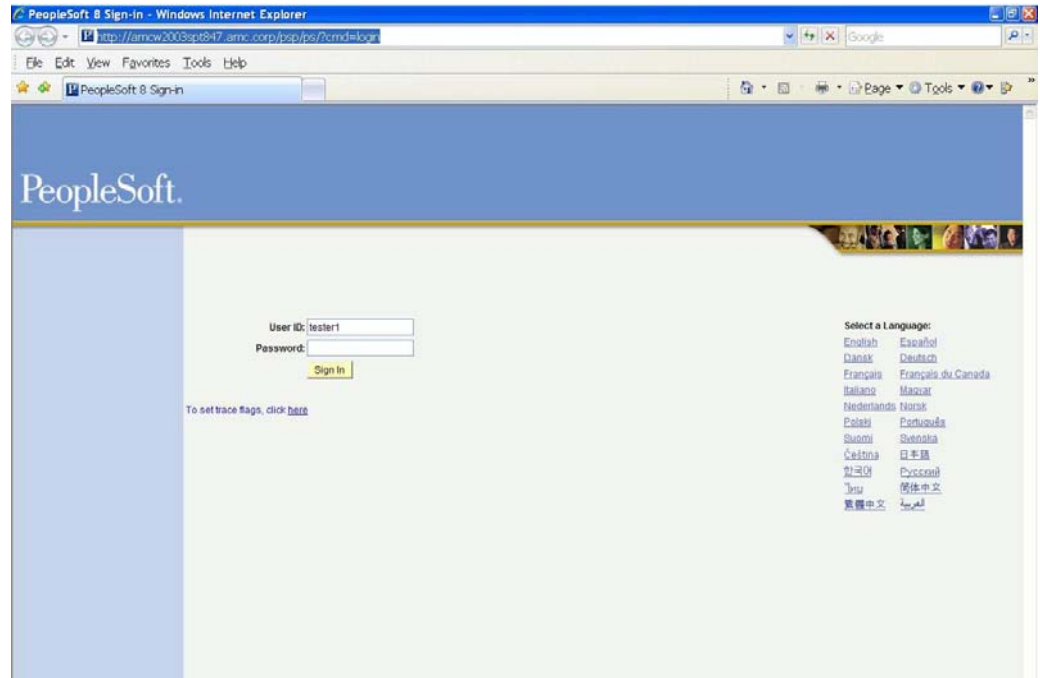
The PeopleSoft Multi-Channel Framework is a web service contact channel integration framework. The first supported version was released as Oracle PeopleTools 8.45. This version includes the Real-Time Event Notification (REN) Server for third party telephony integration. It also includes the Multi-Channel Console (MCC) for call control.

In PeopleSoft Application v8.9 and with PeopleTools v8.45, 8.46, and 8.47 the Multi-Channel Framework only supported telephony for third-party integration. The recent combined release of PeopleSoft Applications v9.0 and PeopleTools 8.48 does support true third-party multi-channel integration. This release has not been validated for the Cisco Application Adapter for PeopleSoft, and the system CRM Connectors only support telephony channels in this first release.

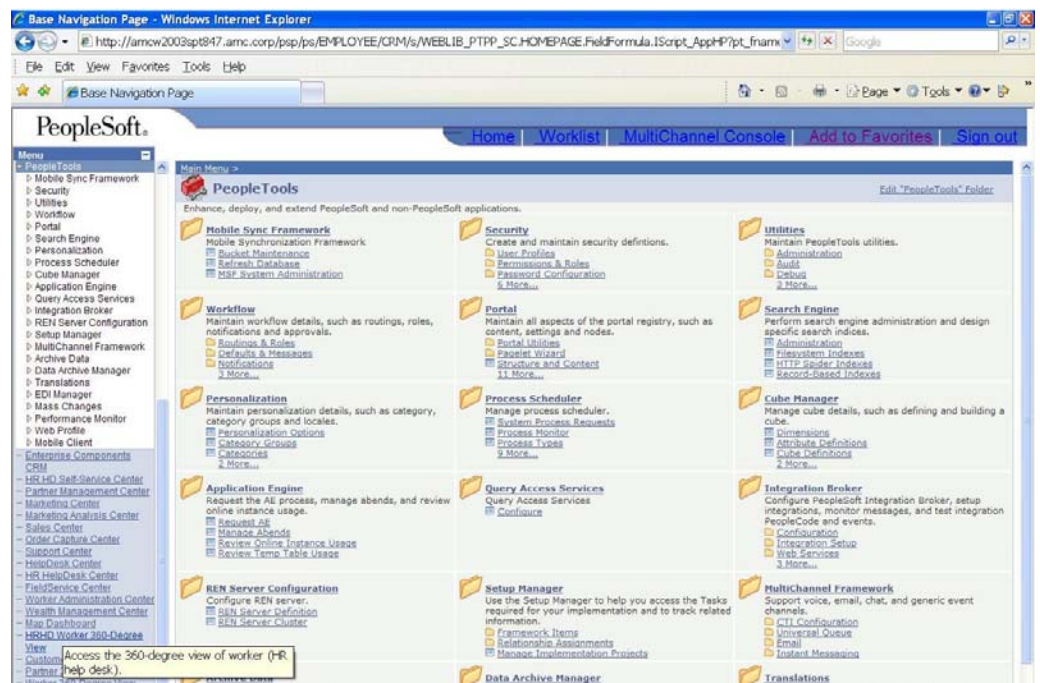
This configuration only provides instructions on how to configure the REN server; the software must first be installed on its host server by a systems administrator.

Log In as PeopleSoft Administrator and Navigate to PeopleTools

Step 1: Log into the PeopleSoft application as a system administrator

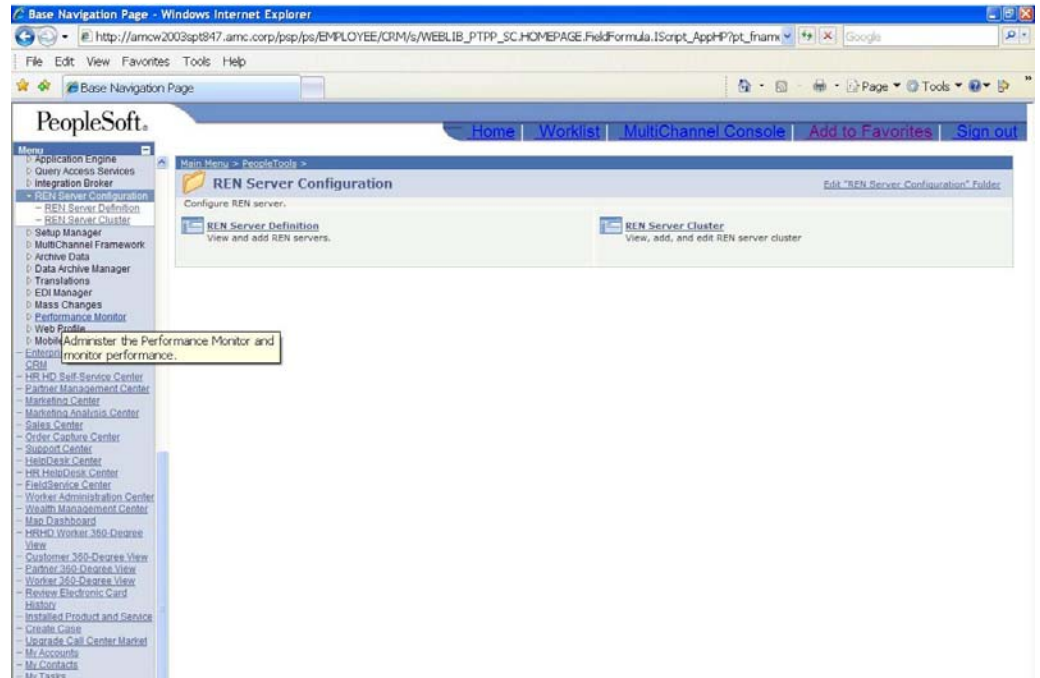


Step 2: Select PeopleTools from the left hand menu bar

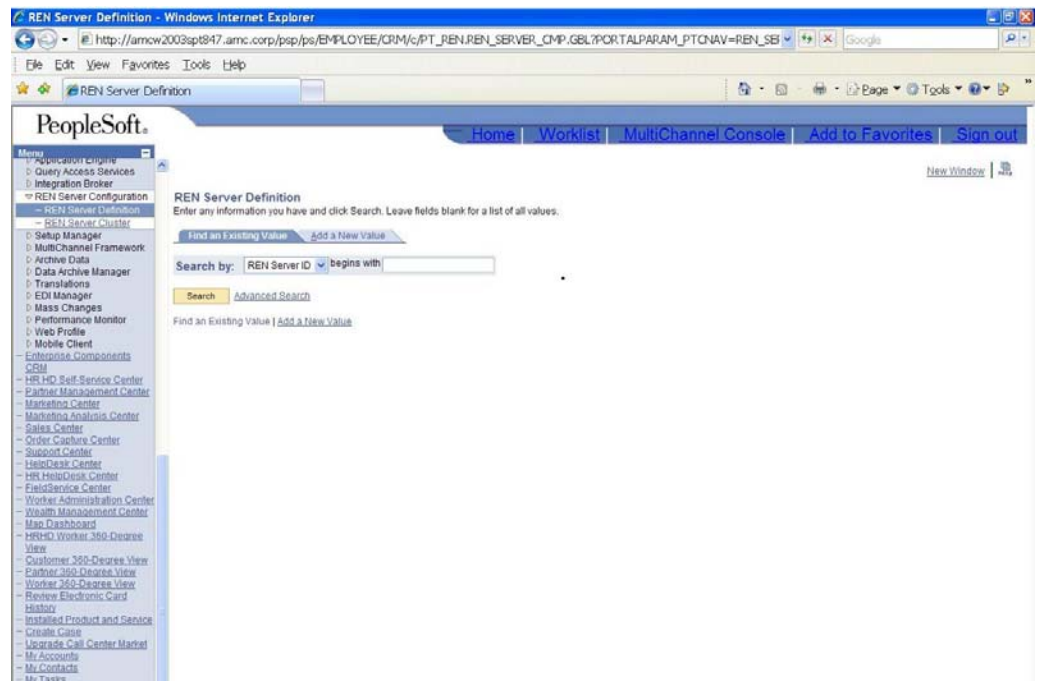


Create a REN Server Configuration

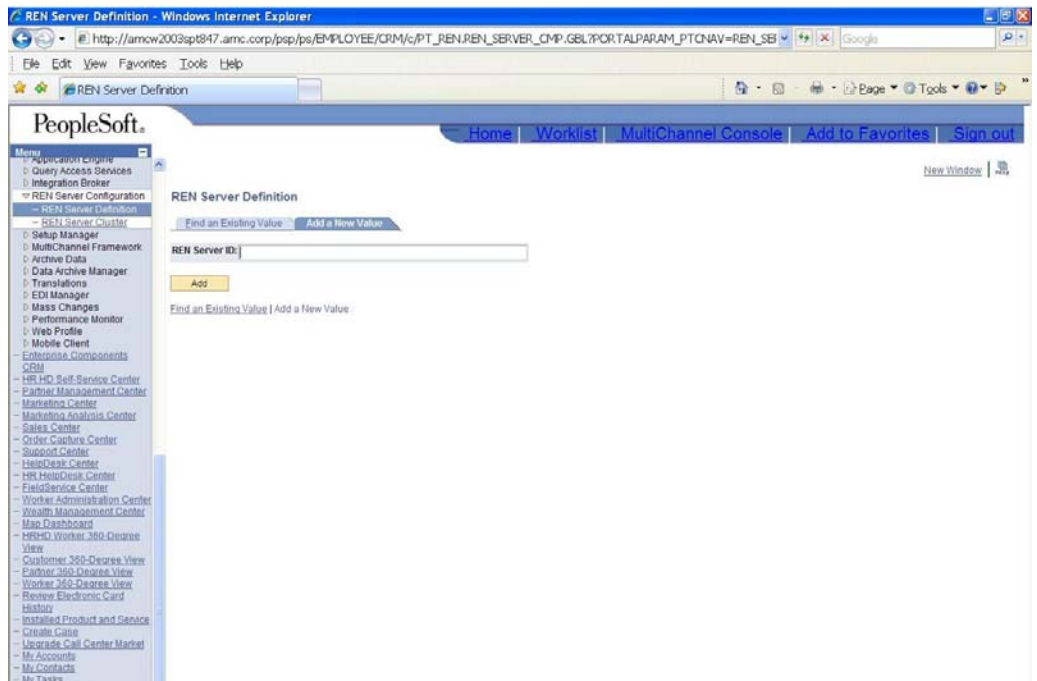
Step 3: Select the REN Server Configuration from the left hand menu bar.



Step 4: Navigate to the REN Server Definition page



Step 5: Select the “Add New Value” tab.

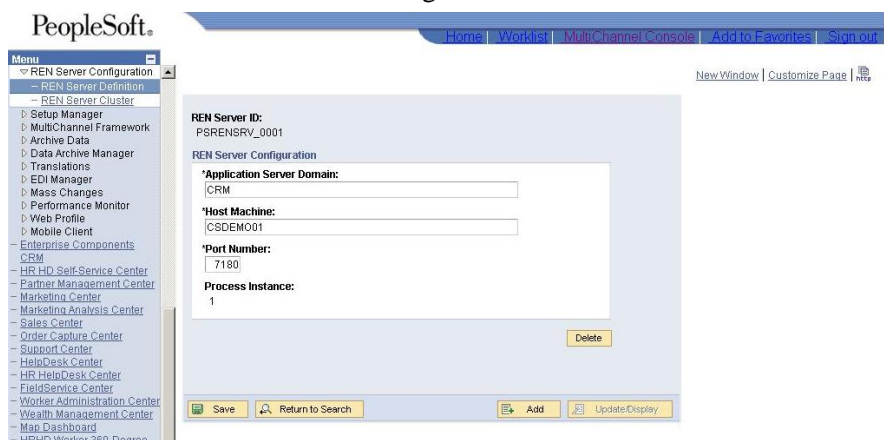


Step 6: Click the “Add” button and add the new REN server configuration information.

Enter the following information:

- The REN Server domain.
- The Host Machine Name or IP Address for the REN Server
- The REN Server listener port number.

Press “Save” to this REN configuration.



Create a REN Server Cluster and test the REN Server

Step 7: Configure a REN Server cluster.

You must configure a REN Server cluster, even if you are only configuring a single REN Server. PeopleSoft provides a REN cluster configuration to provide fail-over. To take advantage of this reliable configuration, the Cisco Application Adapter for PeopleSoft connects to the REN Server cluster.

The screenshot shows the PeopleSoft interface for configuring a REN Server cluster. The left sidebar contains a menu with options like 'REN Server Configuration', 'Setup Manager', 'MultiChannel Framework', 'Archive Data', 'Data Archive Manager', 'Translations', 'EDI Manager', 'Mass Changes', 'Performance Monitor', 'Web Profile', 'Mobile Client', and 'Enterprise Components'. The main content area is titled 'REN Server Cluster' and includes tabs for 'REN Server Cluster Owner' and 'REN Server Cluster Members'. The configuration fields are as follows:

- REN Server Cluster ID:** RENCLSTR_0001
- Cluster Configuration:**
 - State Flag:** Active (dropdown)
 - REN Server Cluster Root Path:** /psren
 - REN Server Cluster URL:** http://CSDemo1.7180 (with a 'Buffer Test' button)
 - REN Server Browser URL:** http://CSDemo1.CISCO.COM:7180 (with a 'Ping Test' button)
 - Authentication Domain:** CISCO.COM

At the bottom, there are buttons for 'Save', 'Return to Search', 'Previous tab', 'Next tab', 'Add', and 'Update/Display'.

Step 8: Enter the REN Server cluster configuration.

You will need to provide the following cluster configuration information:

- The cluster root path. The default is: /psren
- The REN Server Cluster URL: This is the REN server host name (or IP address) and port; e.g., **http://csdemo1:7180**
- The REN Server Browser URL. This is the same as the REN server cluster URL, but adds the domain information; e.g., **http://csdemo1.cisco.com:7180**
- You will need to provide the authentication domain.

This screenshot shows the same PeopleSoft interface as the previous one, but with the 'REN Server ID' field populated. The configuration fields are:

- REN Server Cluster ID:** RENCLSTR_0001
- REN Servers:**
 - REN Server ID:** PSRENSRV_0001

The 'Add' and 'Update/Display' buttons are visible at the bottom.

Step 9: Test the configuration with Ping Test for REN Server and the Buffer Test.

Once this is configured (and the REN server software installed and started) use the PeopleSoft “Ping Test for REN Server” from the REN Server cluster tab: the “Ping Test” Button. Then run the buffer test using the “Buffer Test” button on the same tab.

PeopleSoft.

Ping Test for REN Server

Test Description: This publishes a sequence of ping events to the REN Server, waiting for each to respond before the next publish. Average elapsed time is reported.

Test Conditions: Click on the button below and wait for all 10 pings to complete. Close this window when finished.

Outcome: The test is successful if "Events Sent" and "Events Received" both reach the same final value, and if "Content received" is the same as "Content to send". The average latency depends on network configuration, machine load, and how much debugging is turned on. The PeopleSoft gif in the upper left corner may not transmit through a reverse proxy server; this is normal. Trace messages indicate a problem.

REN Server specified server URL = http://amcw2003spt847.amc.corp:7180/psren

Content to send: Content received:

Events Sent: Trace Messages

Events Received:

Avg Latency (msec):

This is the ping test utility. Enter a test string in the “Content to send” text box and press the “Run Ping Test” button.

PeopleSoft.

Ping Test for REN Server

Test Description: This publishes a sequence of ping events to the REN Server, waiting for each to respond before the next publish. Average elapsed time is reported.

Test Conditions: Click on the button below and wait for all 10 pings to complete. Close this window when finished.

Outcome: The test is successful if "Events Sent" and "Events Received" both reach the same final value, and if "Content received" is the same as "Content to send". The average latency depends on network configuration, machine load, and how much debugging is turned on. The PeopleSoft gif in the upper left corner may not transmit through a reverse proxy server; this is normal. Trace messages indicate a problem.

REN Server specified server URL = http://amcw2003spt847.amc.corp:7180/psren

Content to send: Content received:

Events Sent: Trace Messages

Events Received:

Avg Latency (msec):

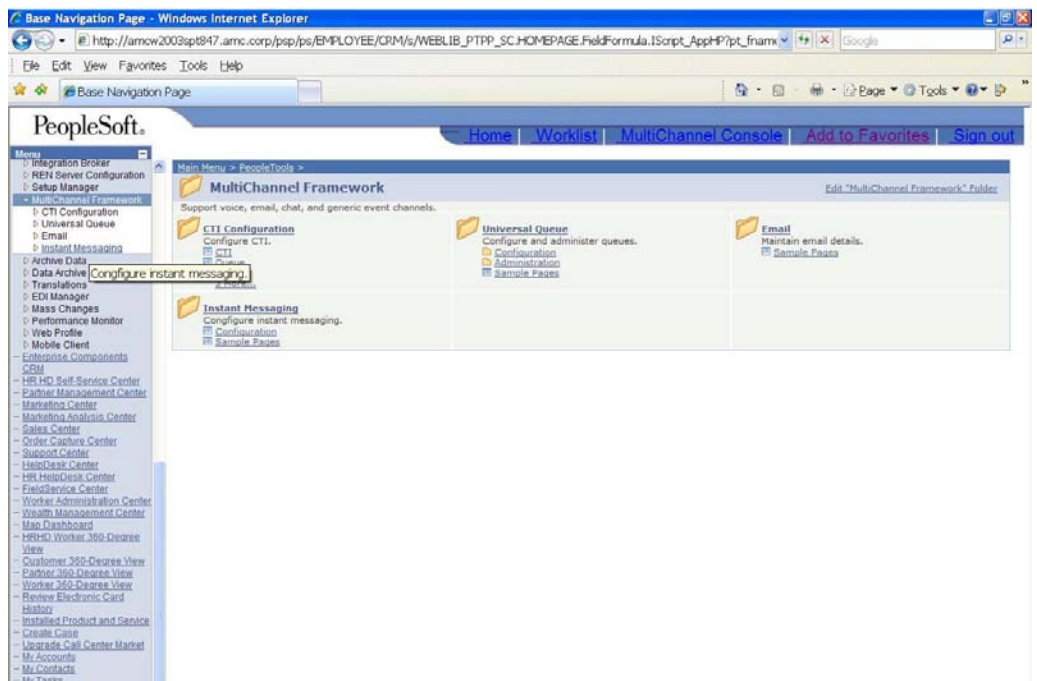
This shows the ping test results in the Content received text box.

This completes configuration of the REN Server

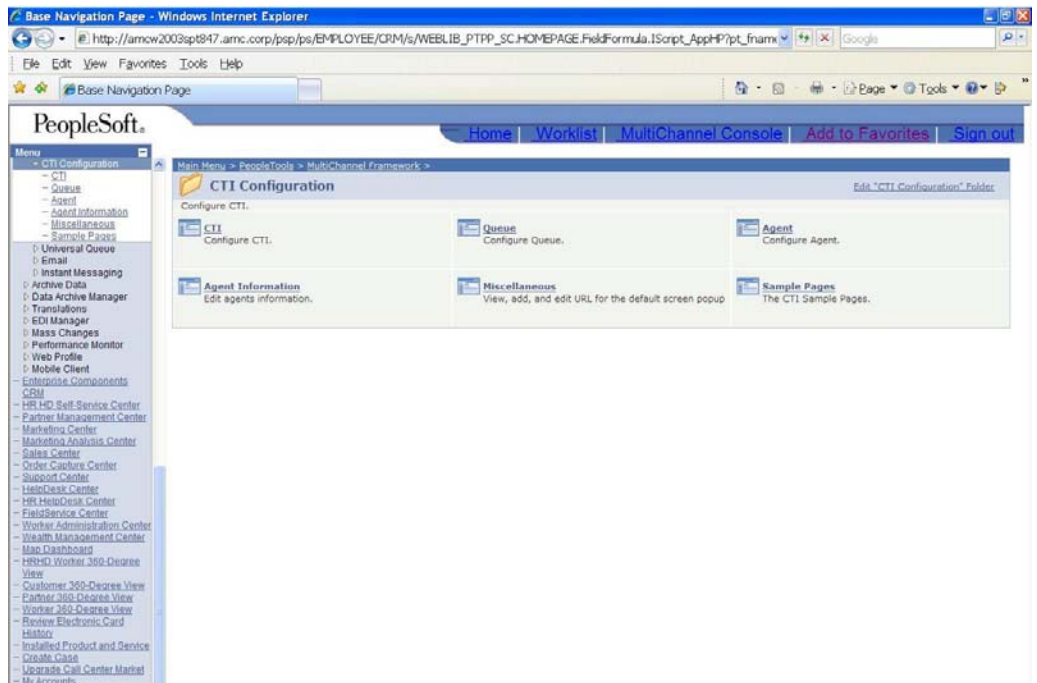
Configure the Multi-Channel Framework Components.

Step 10: Navigate to the Multi-Channel Framework Menu Page

User the PeopleTools menu on left hand menu bar to select the Multi-Channel Framework

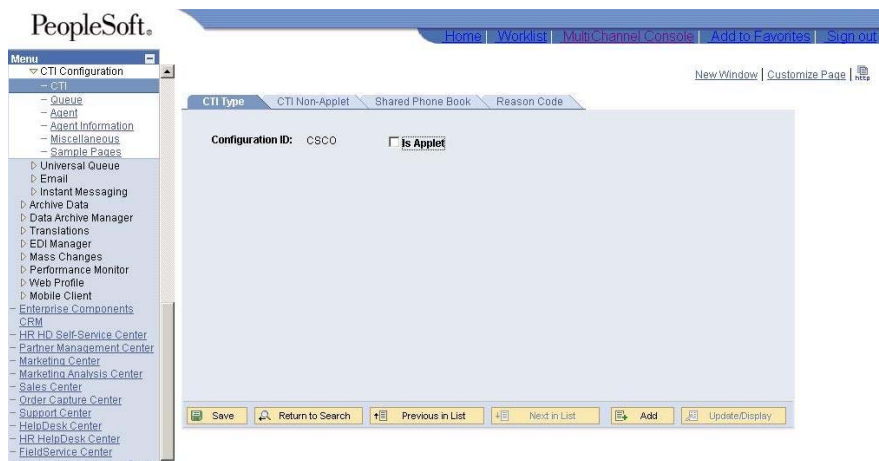


Step 11: Select CTI Configuration to go the CTI Configuration Page



Step 12: Select the CTI link and configure the CTI Type.

On the CTI Type tab enter the CTI type. Click the “Add” button and add the CTI configuration ID “Cisco”. **Do Not Check “Is Applet”**; that option provides backward compatibility for earlier CTI integrations with PeopleSoft.



Step 13: Configure the teleset template on the CTI Non-Applet Tab.

- Enter your chosen adapter name
- Select the REN Server Cluster ID
- Configure the teleset template for
 - 1 Extension
 - 2 Lines
 - 2 Lines on the Console (MCC)

PeopleSoft®

Home | Worklist | Multi-Channel Console | Add to Favorites | Sign out

New Window | Customize Page |

CTI Type | **CTI Non-Applet** | Shared Phone Book | Reason Code

Configuration ID: CSC0

*Configuration Name: CISCO_ADAPTER

*REN Server Cluster ID: RENCLSTR_0001

Number of Extensions: 1

Number of Lines: 2

Lines on Console: 2

Save | Return to Search | Previous in List | Next in List | Add | Update/Display

Step 14: If you choose, you may configure the shared phonebook tab.

This allows certain phone numbers to be shared by agents through a PeopleSoft phonebook: for example a route point or IVR transfer DN.

PeopleSoft®

Home | Worklist | Multi-Channel Console | Add to Favorites | Sign out

New Window | Customize Page |

CTI Type | CTI Non-Applet | **Shared Phone Book** | Reason Code

Configuration ID: CSC0

Phone Book

| *Phone Number | *Type | Description |
|---------------|-------|-----------------|
| 1 2000 | Queue | NORTELE QUEUE 1 |
| 2 3000 | Queue | NORTELE QUEUE 2 |
| 3 4002 | DN | SUPERVISOR ONE |

Save | Return to Search | Previous in List | Next in List | Add | Update/Display

Step 15: If you use reason codes, configure them on the Reason Code tab.

This associates the ACD not ready reason code with a descriptive name. Enter your chosen adapter name

- Enter the Reason Code, the number associated with the not ready reason on the PBX.
- Enter the Reason Message; this is the descriptive name agents will select within PeopleSoft when setting themselves not read.

The screenshot shows the PeopleSoft Reason Code configuration screen. The left sidebar contains a menu with options like CTI Configuration, Queue, Agent, and various centers. The main area is titled 'Reason Code' and shows a table with 5 rows. Each row has a 'Reason Code' field and a 'Reason Message' field. The messages are 'Morning Break', 'Lunch', 'Afternoon Break', 'Personal Emergency', and 'Other Work'. At the bottom, there are buttons for 'Save', 'Return to Search', 'Previous in List', 'Next in List', 'Add', and 'Update/Display'.

| Reason Code | Reason Message |
|-------------|--------------------|
| 1 | Morning Break |
| 2 | Lunch |
| 3 | Afternoon Break |
| 4 | Personal Emergency |
| 5 | Other Work |

Step 16. Configure the supported queues.

PeopleSoft provides a queue definition function. Enter the Queue numbers and a description. **Queues must be defined and assigned to agents.** This associates agents with queues and provides a descriptive name for each queue.

IMPORTANT WARNING: You must define a queue in the PeopleSoft Multi-Channel Framework configuration, even if you do not use queues (or skills) in UCC or the ICM integrated ACD. You may assign a “phantom” queue value, such as 1, 10 or 9999. Agents will not be able to log in without a queue assignment.

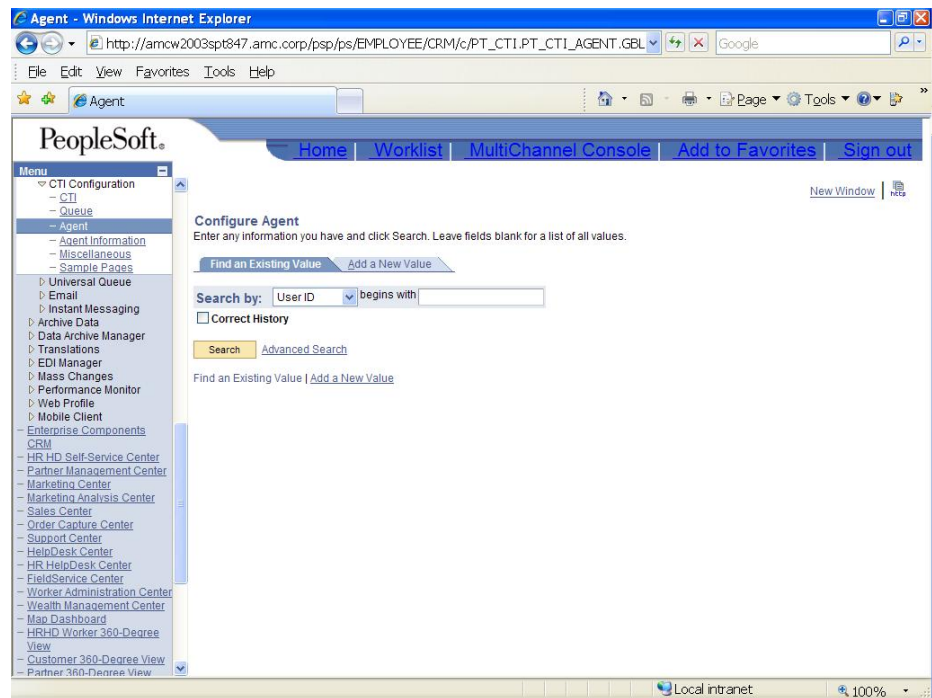
The screenshot shows the PeopleSoft Queue Configuration screen. The left sidebar is the same as in Step 15. The main area is titled 'Queue Configuration' and shows a table with 9 rows. Each row has a 'Queue' field and a 'Queue Description' field. The descriptions are 'IPCC', 'Simulator', 'Nortel', 'IPCCE', 'Avaya', 'Avaya', 'Nortel', and 'Test'. At the bottom, there are buttons for 'Save', 'Return to Search', 'Previous in List', 'Next in List', 'Add', and 'Update/Display'.

| Queue | Queue Description |
|-------|-------------------|
| 1 | IPCC |
| 2 | 10 |
| 3 | 2001 |
| 4 | 2002 |
| 5 | 20061 |
| 6 | 24191 |
| 7 | 24196 |
| 8 | 3000 |
| 9 | 62 |

This completes the multi-channel framework CTI configuration.

Configure agents and assign them to queues and configurations.

Step 17: Select PeopleTools form the left hand menu bar

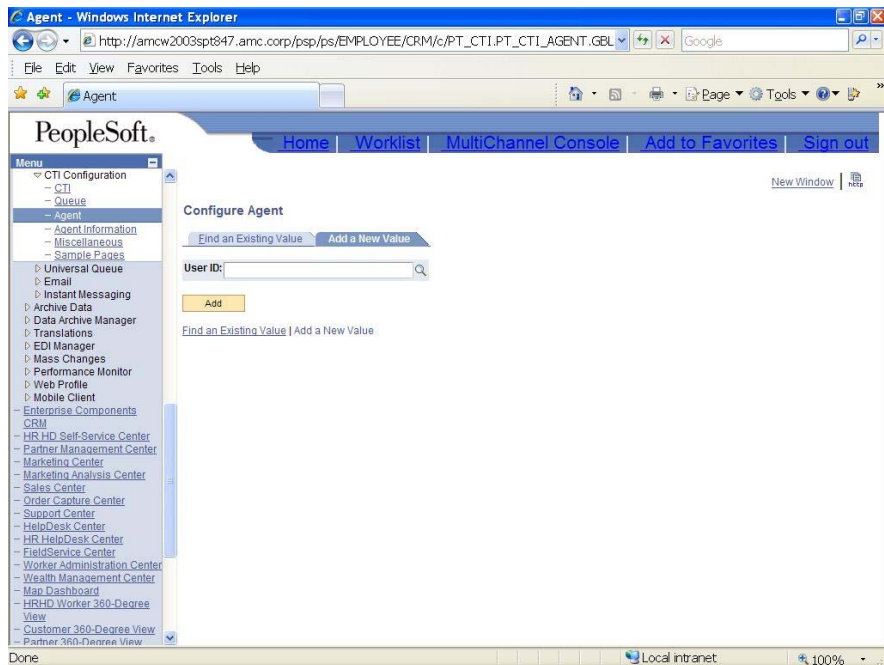


Select "Agent" under PeopleTools → CTI Configuration.

Step 18: Select PeopleTools form the left hand menu bar

On the “Find Existing Value Tab” use the search page to get a list of the configured agents. This lists the agents User IDs and the ACD login, the “CTI Agent ID”

Step 19: Select the Add a New Value tab.



Search for a User ID and hit “Add”

Step 20: Select PeopleTools form the left hand menu bar

Create the agent configuration for the selected user.

- Agent ID is the agents ACD login.
- Agent Password is the ACD login password.
- Queue is the agent’s assigned queue, configured in the earlier queue definition step in Step 16.
- Finally select the agent’s call center configuration. This is the CTI configuration ID defined in Step 14.

PeopleSoft®

Home | Worklist | MultiChannel Console | Add to Favorites | Sign out

New Window | Customize Page |

CTI Agent Configuration | Phone Book | Personalization | Presence | Reason Code

User ID: tester1

Find | View All | First 1 of 2 | Last

Effective Date: 01/08/2008

*Agent ID: 16001

Agent Password: *****

Queue: 1 | IPCC

*Configuration ID: CSCO | CSCO_ADAPTER

*Trace Level: 2 - Debug

Save | Return to Search | Previous in List | Next in List | Add | Update/Display | Correct History

CTI Agent Configuration | Phone Book | Personalization | Presence | Reason Code

IMPORTANT WARNING: You must assign a queue to each agent in the PeopleSoft Multi-Channel Framework configuration, even if you do not use queues (or skills) in UCC or the ICM integrated ACD. You may assign a “phantom” queue value, such as 1, 10 or 9999. Agents will not be able to log in without this queue assignment.

Step 21: Set the Screen Pop “pop-up” mode

This sets the size and position of the pop screen (web browser page). It also set the pop event. There are two choices: “Popup on answer” and “PopUp when incoming.” The application adapter only supports “Popup when incoming.” Other events are not supported.

PeopleSoft®

Home | Worklist | MultiChannel Console | Add to Favorites | Sign out

New Window | Customize Page |

CTI Agent Configuration | Phone Book | Personalization | Presence | Reason Code

User ID: tester1

Popup Window

*Popup Mode: 0 - Popup when incoming

Top: 90

Left: 100

Height: 600

Width: 800

Floating Console

Top: 0

Left: 0

☒ Logout when console is closed

Save | Return to Search | Previous in List | Next in List | Add | Update/Display | Correct History

CTI Agent Configuration | Phone Book | Personalization | Presence | Reason Code

This completes the configuration steps for the PeopleTools Multi-Channel Framework

Installing the Cisco Application Adapter for Oracle PeopleSoft

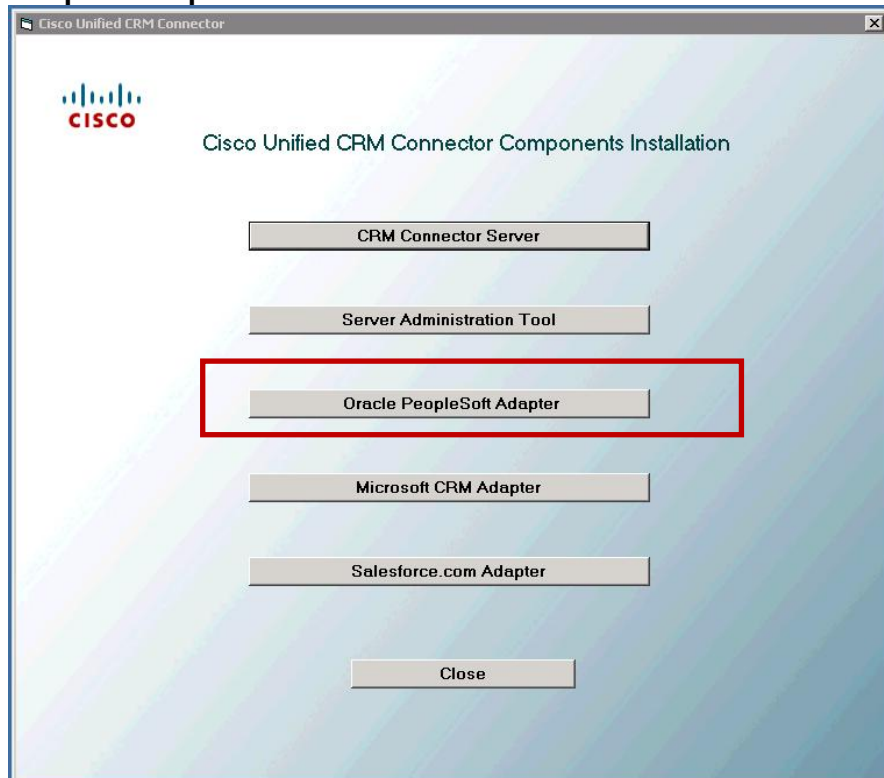
This section describes the software installation process for the PeopleSoft application adapter.

Be sure you have:

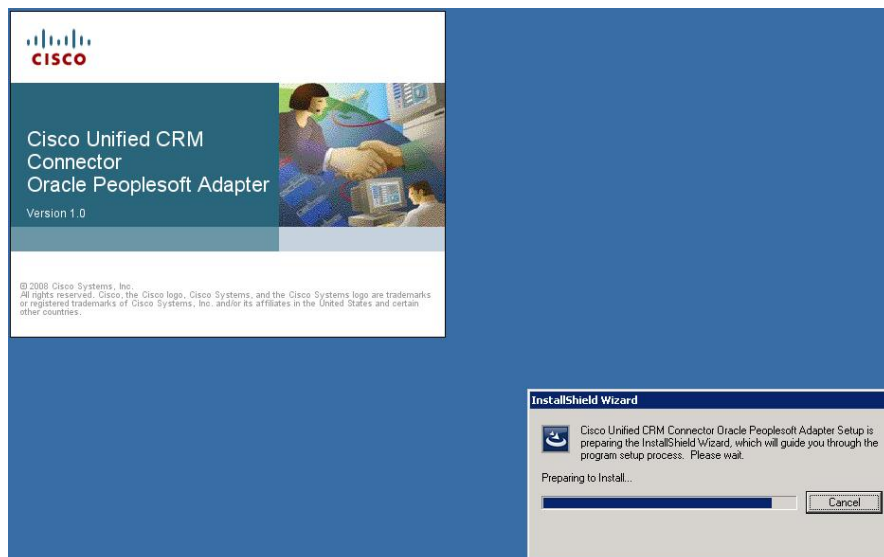
- The REN Server URL information.

- The host name of the CRM Connector Server machine.
- Installed the JRE and the .NET Framework V2.0 on the adapter server.

Step 1: Start the installation and select the Oracle PeopleSoft Adapter component.

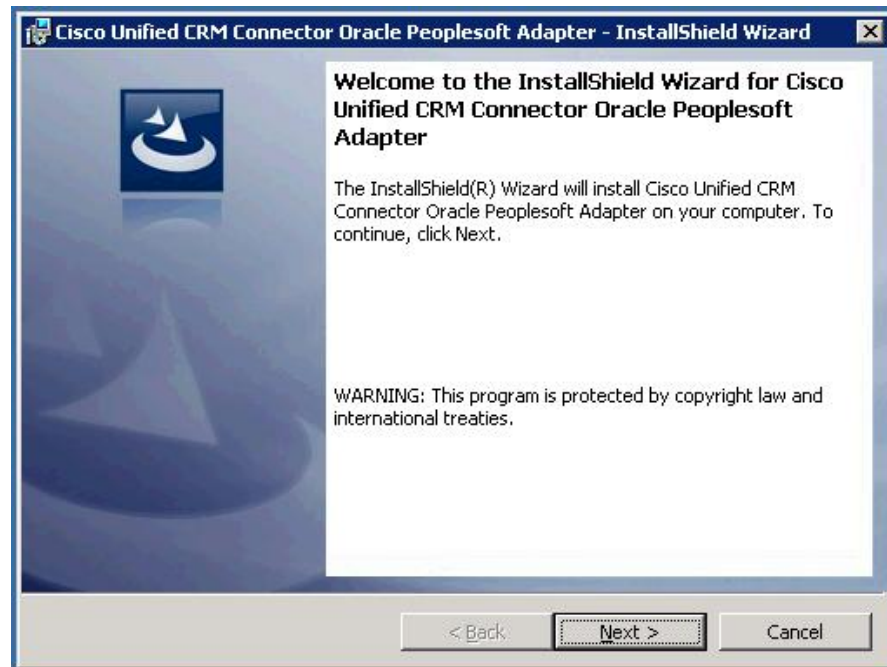


- The install starts and displays the splash screen.



Step 2: Start the install and accept the End User License Agreement.

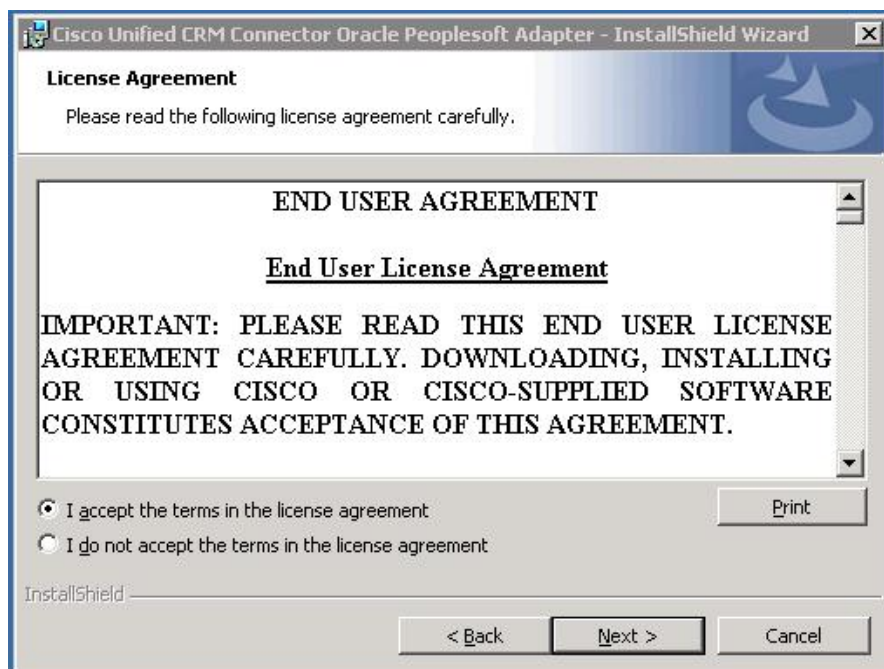
- The install launches the InstallWizard that displays the welcome dialog. Press *Next* to start the installation process.



- The installer next displays the End User License Agreement (EULA)

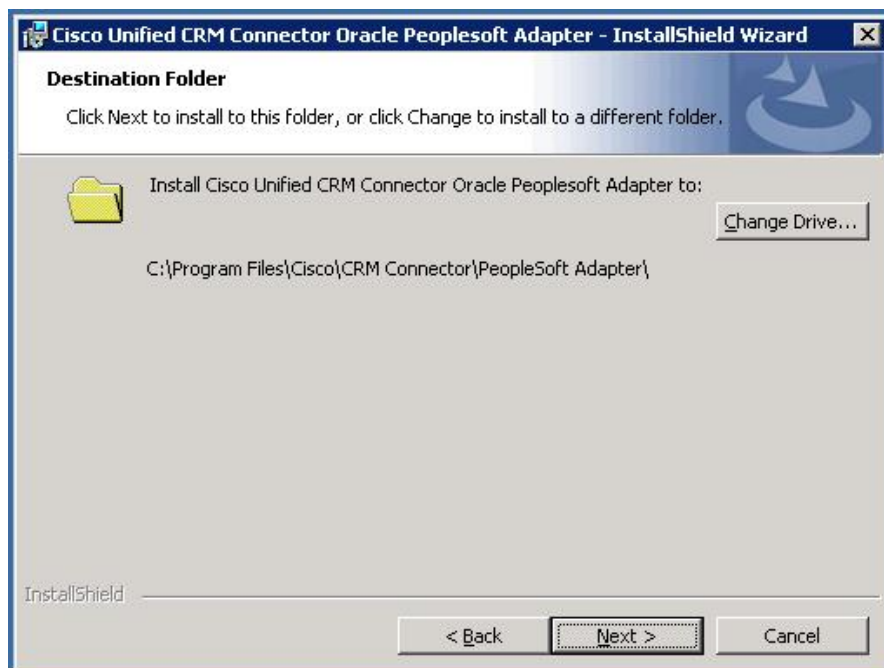


- Read the agreement and click the "accept" radio button. This will enable the "Next" button.

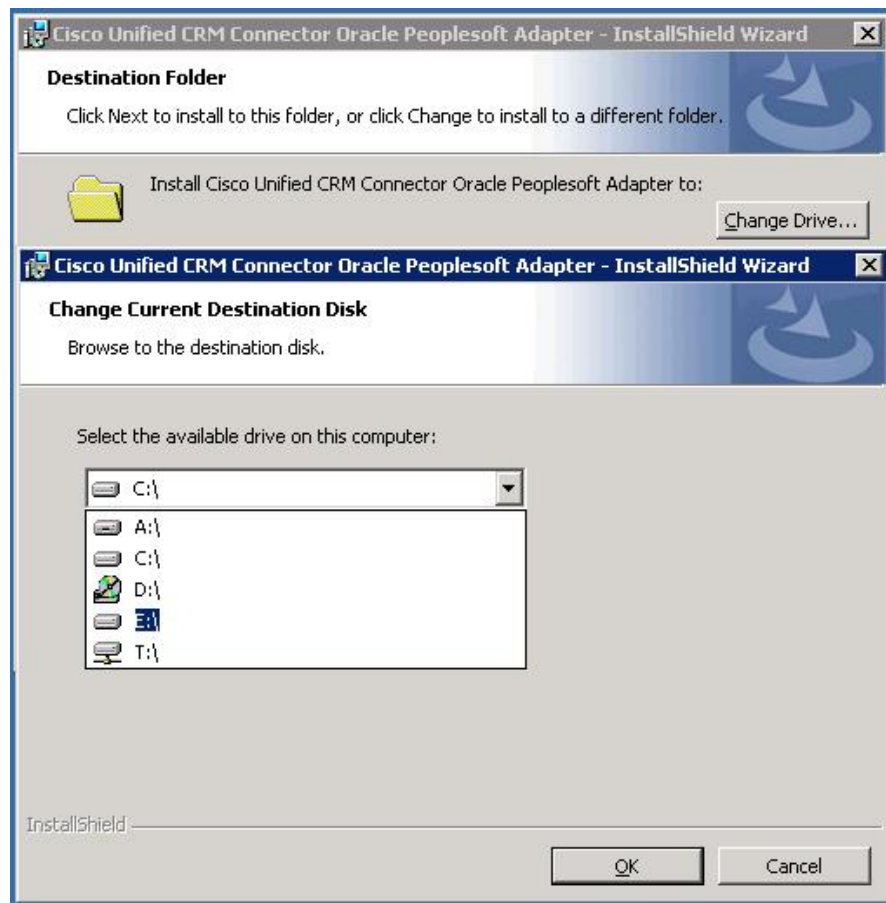


Step 3: Select the target installation drive.

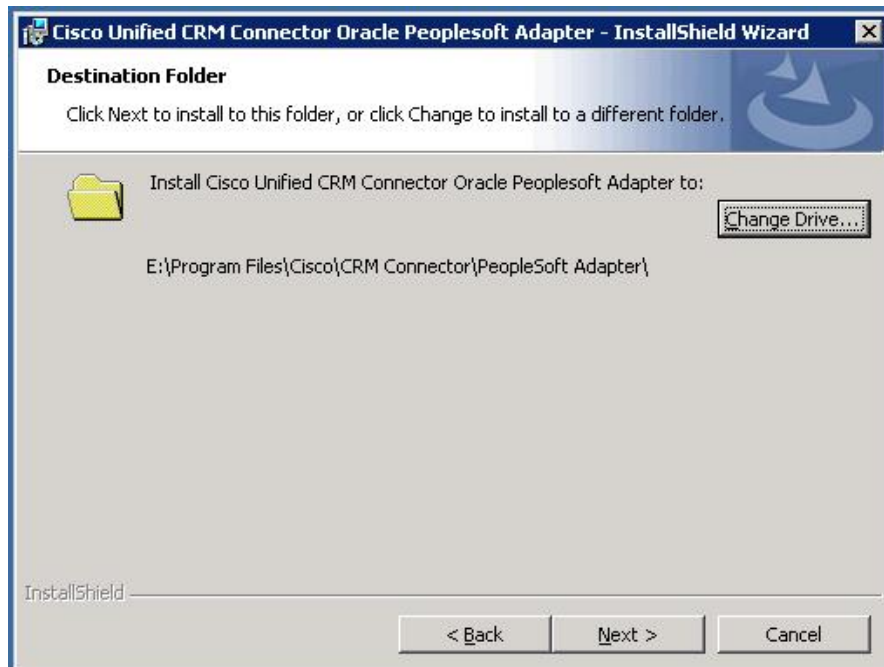
- The change drive dialog allows you to select the drive where the adapter will be installed.



- By default the software installs on the C: drive; use the Change Drive button to select another drive on this server.



- Use the drop down on the Choose Destination Drive page to list the available install drives. Once you have selected a drive, Press OK



- This returns to the Change Drive dialog. Press "Next" to continue installing the adapter.
- The installation continues prompting for configuration information; this will be used to build the PeopleSoft Adapter Configuration file.
- Accept the default information, but in the REN add the REN server host name or IP address; be sure to leave the rest of the URL untouched.
- Press "Next" to continue.

Step 4: Configure the PeopleSoft Adapter Settings.

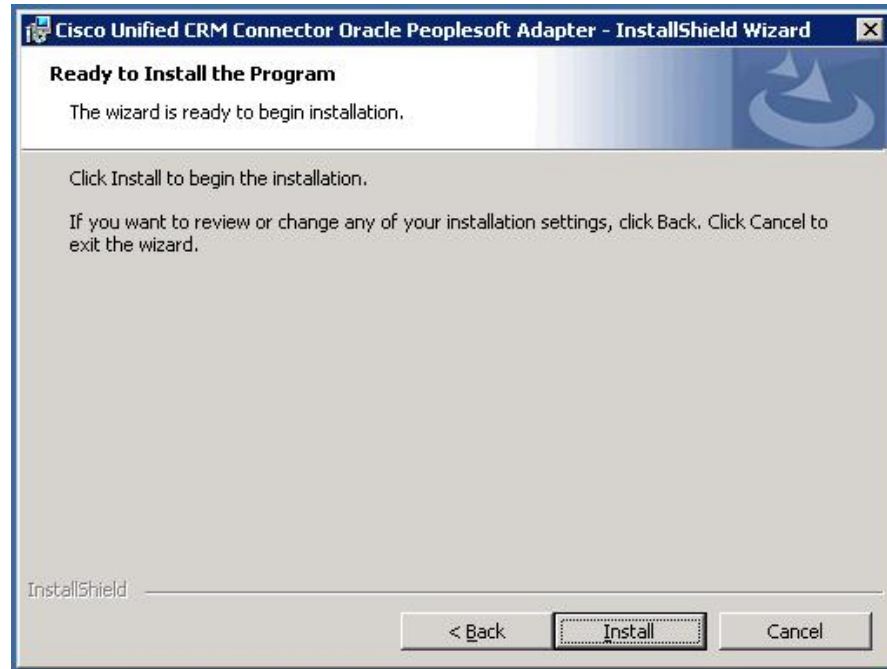
The screenshot shows a Windows-style dialog box titled "Cisco Unified CRM Connector Oracle Peoplesoft Adapter - InstallShield Wizard". The "Edit Data" tab is selected, and the instruction "Enter Requested Data" is displayed. Below the instruction, a message states: "Please configure PeopleSoft parameters for the Application Adapter:". There are three text input fields: "Provider ID" with the value "CISCO", "REN Server URL" with the value "http://REPLACE_HOSTNAME.DOMAIN.CORP:7180/psren", and "System Info" with the value "ciscoAdapter". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The "InstallShield" logo is visible in the bottom left corner.

- Next the installer prompts for web service connection information. Enter the CRM Connector server host name and port in the first line text box. This is the CRM Connector Server host name or IP address.
- This uses the well-known HTTP port; it must be supported by your IIS server configuration. IIS server may be configured either for 8080 or 80; if 8080 is not supported, then use port 80.
- Press Next to continue.

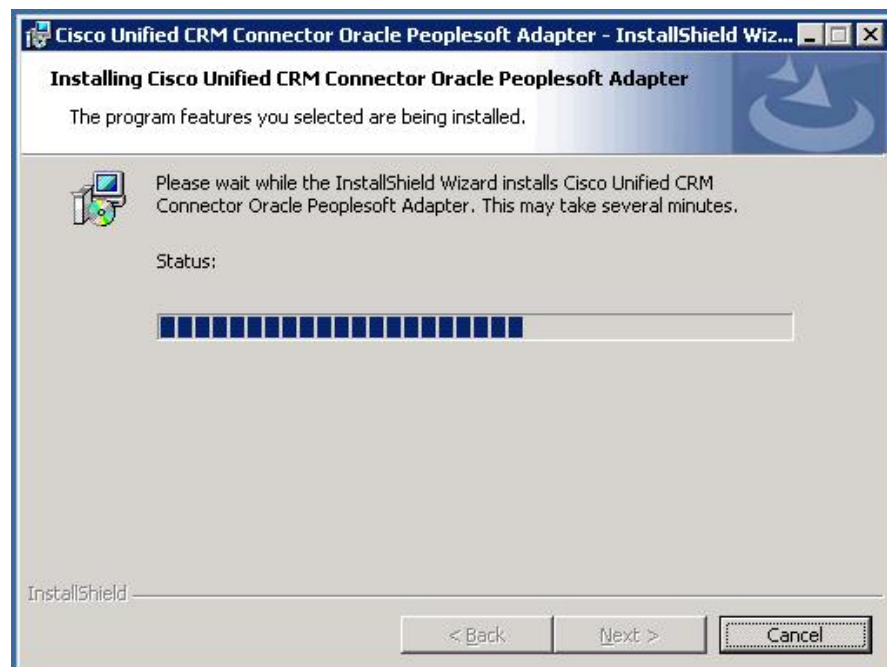
The screenshot shows the same dialog box as above, but with different values in the text input fields. The instruction "Enter requested data." is displayed. The message states: "Please configure CRM Connector Server parameters for Oracle PeopleSoft Adapter:". There are three text input fields: "Server Host Name:Port" with the value "REPLACE_HOSTNAME:80", "WebService Request Folder" with the value "AMCDotNetAdapterWebService", and "WebService Event Folder" with the value "AMCDotNetEventAdapterWebService". At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The "InstallShield" logo is visible in the bottom left corner.

Step 5: Install the software and finish the installation.

- The installer will now install the software; the installer displays the “Ready to install” dialog. Press “Install” to continue.



- This displays the progress dialog.



- This displays the finished dialog. Press “Finish” to exit the installation.

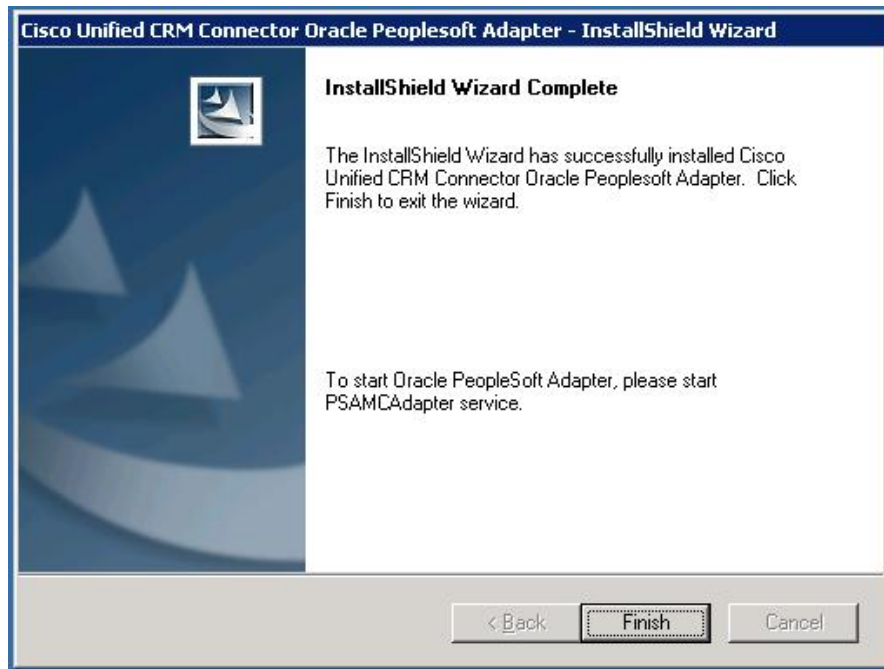


Table 8-1: PeopleSoft Adapter Directory Structure shows the PeopleSoft Adapter directory structure.

Table 8-1: PeopleSoft Adapter Directory Structure

| Sub-Directory | Component | Use |
|---|-----------------|--|
| F:\Program Files\Cisco\CRM Connector | | This is the parent drive location; all agent desktop application adapters will be installed under this directory hierarchy. |
| F:\Program Files\Cisco\CRM Connector\PeopleSoft Adapter | | This is the application adapter parent directory. |
| | PSAMCAdaper.exe | <p>This is the PeopleSoft Adapter service. It is installed as a service and runs under the system account.</p> <p>The service name is PSAMCAdapter</p> <p>This service is used to control the PSMCAPI adapter and its Java machine. Starting the service launches the PSMCAPI adapter; stopping it shuts down the adapter.</p> <p>Note that this service cannot be controlled using the Administration Tool. You must use the Services manager.</p> |
| F:\Program Files\Cisco\CRM Connector\PeopleSoft Adapter\bin | | <p>This directory holds all of the PSMCAPI adapter JAR files. (Java archive files).</p> <p>It also holds the configuration file and PeopleSoft specific log files and</p> |

| Sub-Directory | Component | Use |
|--|-------------------|--|
| | | configuration settings files for the PSMCAPI adapter. |
| | PSAMCAAdapter.jar | This is the Cisco PeopleSoft application adapter Java component. |
| | Psmcapi.jar | This is the PeopleSoft psmcapi Java file. Cisco includes this to ensure core operation of the adapter. You may wish to replace this with the version of PSMCAPI.JAR for your version of PeopleTools. |
| F:\Program Files\Cisco\CRM Connector\PeopleSoft Adapter\logs | | <p>This is the log file directory for the PeopleSoft adapter; note that this is a different directory from the CRM Connector logs directory.</p> <p>The PeopleSoft application adapter is designed as a stand-alone install.</p> |

Configuring the Cisco CRM Adapter for Oracle PeopleSoft

Once the software is installed you will need to configure the application adapter. The PeopleSoft application adapter uses an XML format file in the bin sub-directory under the PeopleSoft adapter parent. This file is named “CONFIG.XML” it was partially configured in the last two dialog prompts of the install.

To complete configuring the application adapter you will add PeopleSoft user credentials. These are used to log into the REN server. Example 8-1: PeopleSoft Adapter Config XML File shows the full config.xml file.

Table 8-2: PeopleSoft Adapter Configuration Settings shows the XML file configuration settings. The “parameter” name is the XML tab name (between the angle brackets) and the value is the information sandwiched between the start and end tag parameters.

Many of these parameters are fixed however some must be configured before the PeopleSoft Adapter will work.

Table 8-2: PeopleSoft Adapter Configuration Settings

| Parameter Name | Valid Values / Default | Use |
|----------------|--|--|
| TraceLevel | ERROR WARNING INFO DEBUG Default = DEBUG | The log file trace level. |
| LogPath | The log subdirectory under the application adapter parent. | This is the log file directory. You may change this if you wish. |
| RENServer | REN Server URL | This is the url used to access the REN Server. This was configured as part of the install. If this |

| Parameter Name | Valid Values / Default | Use |
|--------------------|------------------------|--|
| | | changes you may update this with the new URL. |
| CTIUserID | | This is the REN Server log in account. Replace this with an authorized account with privileges to log into the REN Server. The adapter will not work if this account cannot log in. |
| CTIUserPW | | This is the password for the CTIUserID account. |
| TelephonyChannelID | CTI1 | This is the telephony channel ID. It must match the CTIModule value. |
| DataStore | DataStore | This is the data store configuration used by the adapter. |

Example 8-1: PeopleSoft Adapter Config XML File

```

<?xml version="1.0" encoding="UTF-8" ?>
- <root>
- <!--
  ApplicationAdapter params
  -->
  <TraceLevel>DEBUG</TraceLevel>
  <LogsPath>d:\Program Files\Cisco\CRM Connector\PeopleSoft Adapter\LOGS\</LogsPath>
  - <!--
    PeopleSoft params
    -->
    <Provider>AMC</Provider>
    <RENServer>http://admndev006.wrk.ads.pha.phila.gov:7180/psren</RENServer>
    <CTIUserID>ctiuserid</CTIUserID>
    <CTIUserPW>ctiuserpw</CTIUserPW>
    <ServerID>amcServer</ServerID>
    <SystemInfo>amcAdapter</SystemInfo>
  - <!--
    MCIS params
    -->
    <MCISHost>PHAAMC01:8080</MCISHost>
    <WebServiceRequestFolder>AMCDotNetAdapterWebService</WebServiceRequestFolder>
    <WebServiceEventFolder>AMCDotNetEventAdapterWebService</WebServiceEventFolder>

```



```
<TelephonyChannelID>CTI1</TelephonyChannelID>
<DataStore>IDataStore</DataStore>
<WorktopManagementFile>WorkTopManagement.asmx</WorktopManagementFile>
<TelephonyServicesFile>TelephonyServices.asmx</TelephonyServicesFile>
<ContactManagementFile>ContactManagement.asmx</ContactManagementFile>
<CADManagementFile>ContactAssociatedDataManagement.asmx</CADManagementFile>
<EventMode>FILTER</EventMode>
<EventTimeout>5</EventTimeout>
- <!--
  CTI specific
-->
<CAN_LOGIN>YES</CAN_LOGIN>
<CAN_SET_WORK_READY>NO</CAN_SET_WORK_READY>
<CAN_SET_WORK_NOT_READY>NO</CAN_SET_WORK_NOT_READY>
<CAN_SET_PRESENSE>NO</CAN_SET_PRESENSE>
<CAN_REFRESH_STATE>NO</CAN_REFRESH_STATE>
</root>
```

9. IMPLEMENTING THE MICROSOFT CRM ADAPTER

Purpose

This chapter describes the procedures to implement the Cisco Adapter for Microsoft CRM. Microsoft CRM does not have a channel integration framework. Therefore this adapter extends the Microsoft CRM application with administration utilities and the Cisco Contact Center.

The Cisco Contact Center is a web-page form agents use to receive and manage customer contacts. It enhances Microsoft CRM, adding telephone control, agent channel session management and customer screen-pop and interaction control.

This chapter covers:

- Pre-installation Requirements. This adapter has an extensive list of pre-requisite software.
- Installing and configuring the Microsoft CRM Adapter.
- Administering the Microsoft CRM Adapter.

See also the agent user's guide for the Microsoft CRM: *Cisco Adapter for Microsoft CRM 3.0 Users Guide*

Overview: Implementation Process Steps.

Before performing any installation or implementation work you should read this entire chapter. This section lists the implementation process steps; later sections provide step-by-step implementation instructions.

- Implement both the Cisco CRM Connector Server and the Cisco CRM Connector for UICM, UCCE and UCCH.
- Create two configurations, one to support off-line tests using the Null CTI Server and the other for Cisco CRM Connector for UICM, UCCE and UCCH.
- Configure the .Net Adapter for Soap web services.
- Install the Cisco Microsoft CRM Adapter on the Microsoft CRM server.
- Configure web settings in web.config files.
- Use the Cisco Contact Center administration web-pages to configure general settings such as known queues, favorite numbers, screen pop search criteria, and reason codes.
- Configure agent specific settings such as queue assignments, favorites, channel assignments and extension and ACD logins.

- Perform optional MS CRM customization for CRM Adapter users.

This implementation varies from the other Cisco adapter implementations. The Microsoft CRM Adapter extends the Microsoft CRM application to include administration tools and an agent user interface, the Cisco Contact Center, which allows agents to receive screen pops, manage their calls and control their channel work sessions.

Pre-Installation Requirements

The Cisco CRM Adapter for Microsoft CRM 3.0 is installed upon the Microsoft CRM server. It extends the Microsoft CRM application with new menu options and web-page forms that serve as administrative and agent user interfaces.

What you will need.

Microsoft CRM User Account

Installation requires a Microsoft CRM user account with administration privileges. You will need account credentials to complete the installation. The account becomes the “owner” of the Microsoft CRM application extensions. It will also be used to administer contact center configurations and agents.

SQL Server Account

Installation requires an SQL Server account with schema create, modify and delete privileges. This account will be used to create and own the application adapter schema.

A SQL Server account with full access rights on the CRM application adapter schema is also required to access the database on behalf of application adapter web services. This can be the same account or a different account. By default, the installation configures the installation database credentials for web services access.

As part of the installation, The Cisco adapter installs a data schema in the Microsoft CRM SQL Server instances.

Supported Operating Systems and Environments

- The Cisco CRM Adapter for Microsoft CRM 3.0 has the same operating system requirements as the Microsoft CRM system.
- Windows patches should be up-to-date before installing the adapter.
- It may be installed upon the same Microsoft IIS used for Microsoft CRM system.
- The data schema may be installed upon the same SQL Server instance used for the Microsoft CRM system.

Table 9-1: Summary of Required Software

| Software Name and Version | Part of Installation | Additional Information |
|------------------------------------|----------------------|--|
| Operating Systems: Windows 2003 | No | Windows operating systems must be purchased and installed separately. |
| .Net Framework version 2.0 | Yes | The installer will install this if it is not present. Download it from the Microsoft Download Center. |

Pre-installation steps

Step 1: Implement Cisco CRM Connect Server.

CRM Connector Server must be installed, configured and operational before you implement any additional CRM Connector components.

Step 2: Implement the Cisco CRM Connector for Unified ICM and Unified Contact Center Enterprise and Hosted and the Null CTI Connector configuration for initial testing.

You should have configurations that support both the live Cisco CRM Connector and the Null CTI connector. This will allow testing the application adapter independently of other connection and CTI considerations before testing with live CTI.

Once the application adapter installation is confirmed using the Null CTI Connector, use the Cisco CRM Connector for live phone call tests.

You may create this configuration using separate config.ini files, by commenting out the Cisco CRM Connector while testing the Null connector, or with separate CTIModules, one for the Null CTI Connector and another for the live Cisco CRM Connector.

Step 3: Make sure no web site is using Port 81 on the Microsoft Internet Information Server (IIS).

The Microsoft CRM 3.0 Adapter uses Port 81. If a CRM Connector component is also configured on this port it will cause a conflict.

Installing the CRM Adapter for Microsoft CRM 3.0

This section provides step-by-step instructions on installing the CRM Adapter for Microsoft CRM 3.0 on the Microsoft server.

Step 1: Start the Cisco installer

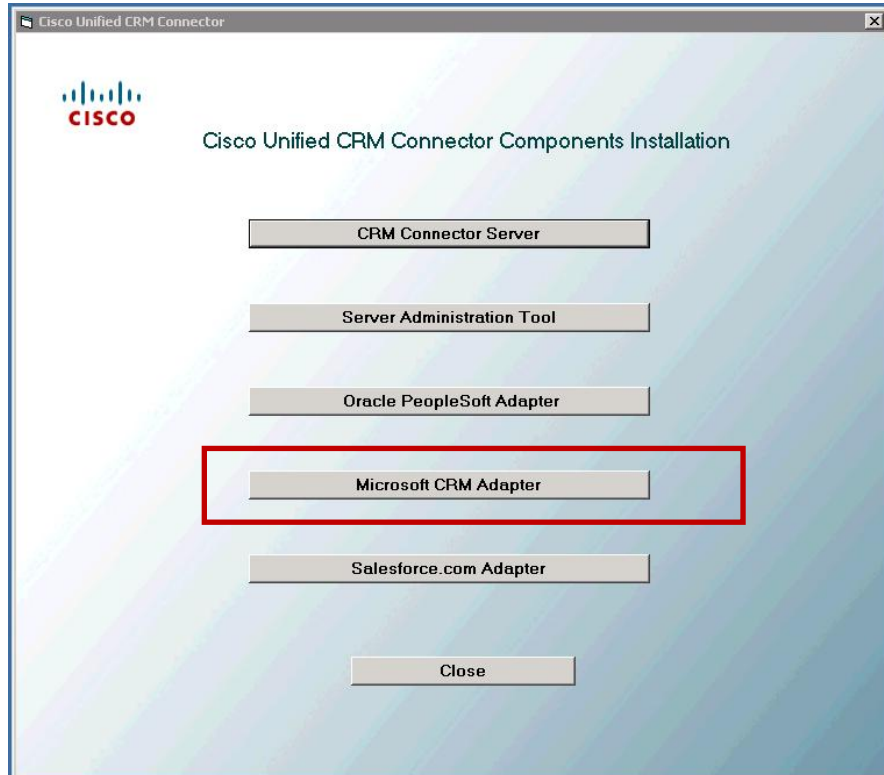
Log into the Microsoft CRM 3.0 Server.

You must install the CRM Adapter for Microsoft CRM on the Microsoft CRM server. Log in using an account that has local system administration privilege on the server **and** administrator privileges within Microsoft CRM.

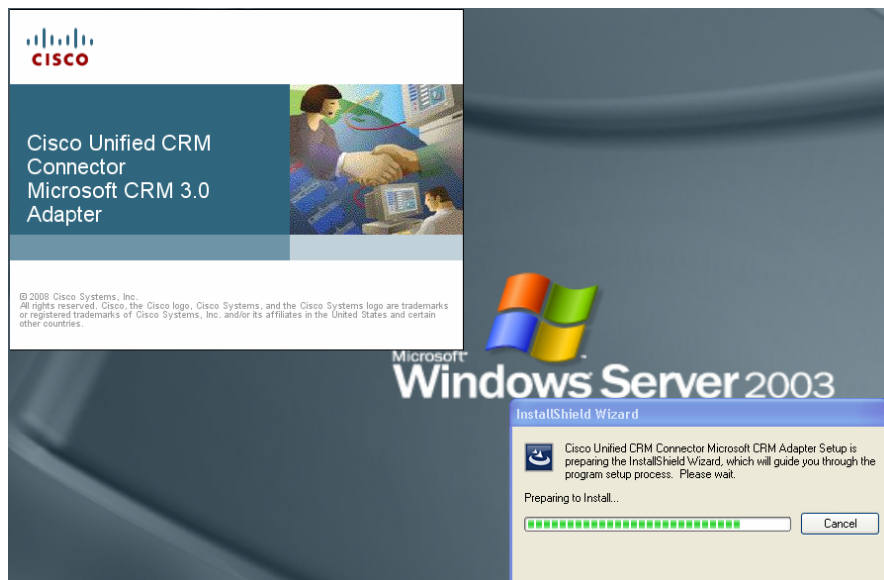
Note: Optionally, you may log on using an account without administrator Microsoft CRM privileges. You will then need to authenticate yourself to the Microsoft CRM application with administrator credentials in order to complete the installation. In general the installation goes more smoothly if

you log in using a single account that has Microsoft CRM administration privileges.

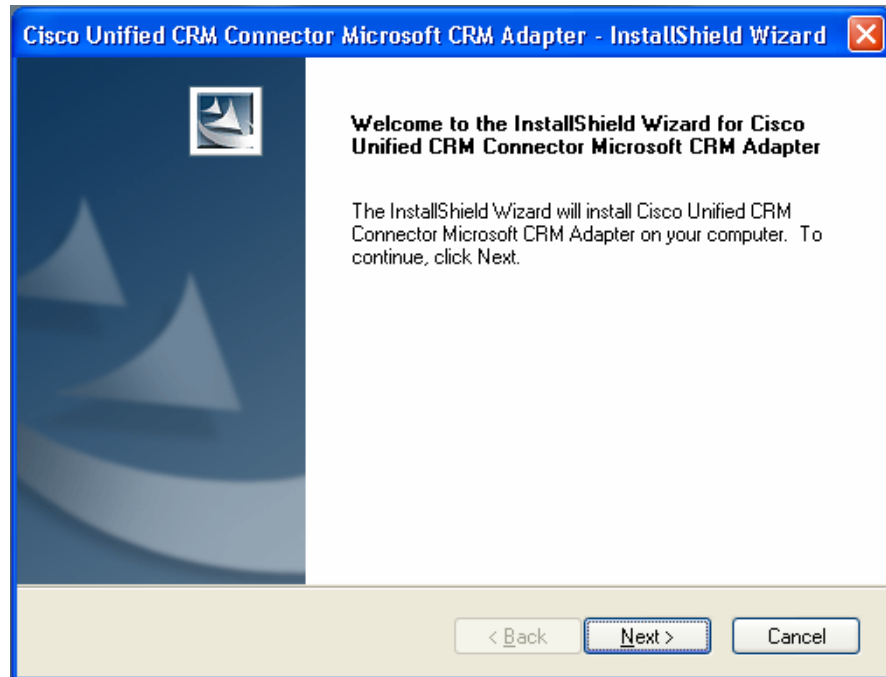
Launch the Installer and select the Microsoft CRM Adapter



- This will launch the Installation Wizard and display the splash screen and then display the InstallShield Wizard welcome screen.



Step 2: Accept the license agreement and installation drive.



- If you have not already installed .Net Framework 2.0, the install wizard will launch the .Net Framework 2.0 installation.
- Press **Next to continue the installation.**
- You are prompted with the End User License Agreement (EULA).

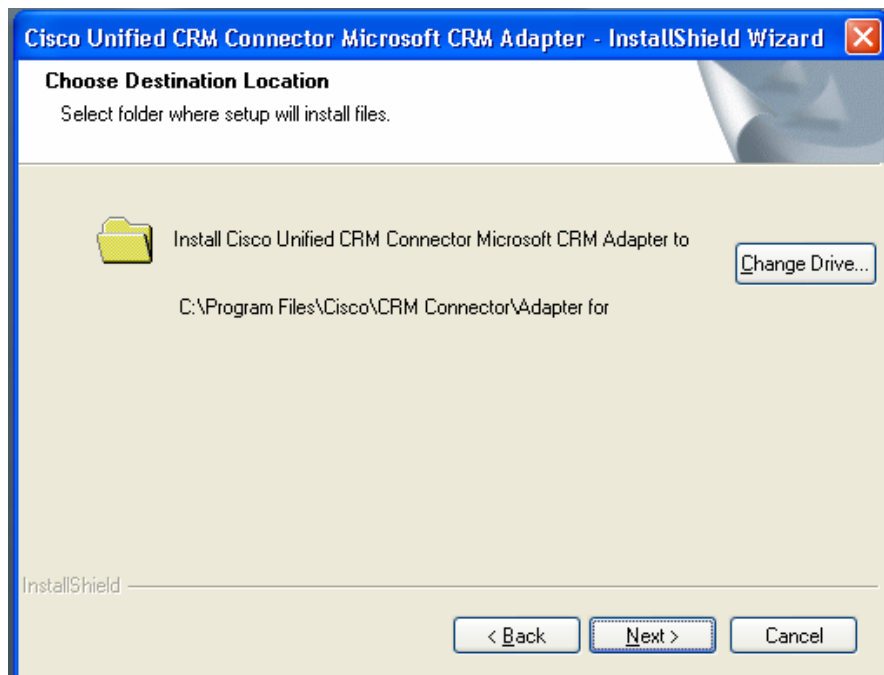


- **Read and Accept the license agreement.**

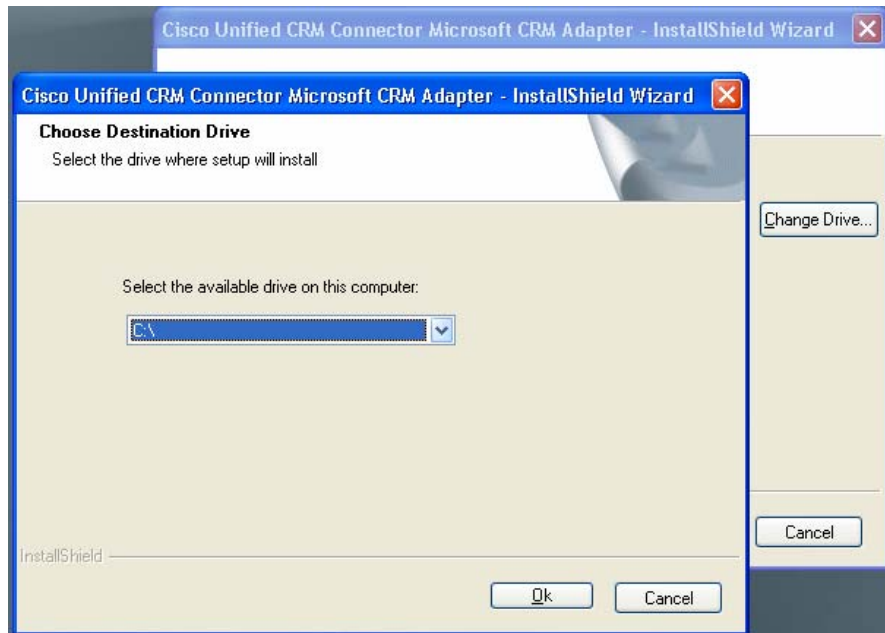
- After reading the EULA, press the “I accept...” radio button. You must accept the agreement to enable the Next button and continue the installation.



- Press Next to start the installation.
- You are prompted to select the target installation drive. Use the Change Drive button if you do not want to install the adapter on the system driver (usually the C:\ drive).



- To change drives, select the “Change Drive” button.
- Pressing change drive opens the Choose Destination Drive dialog:



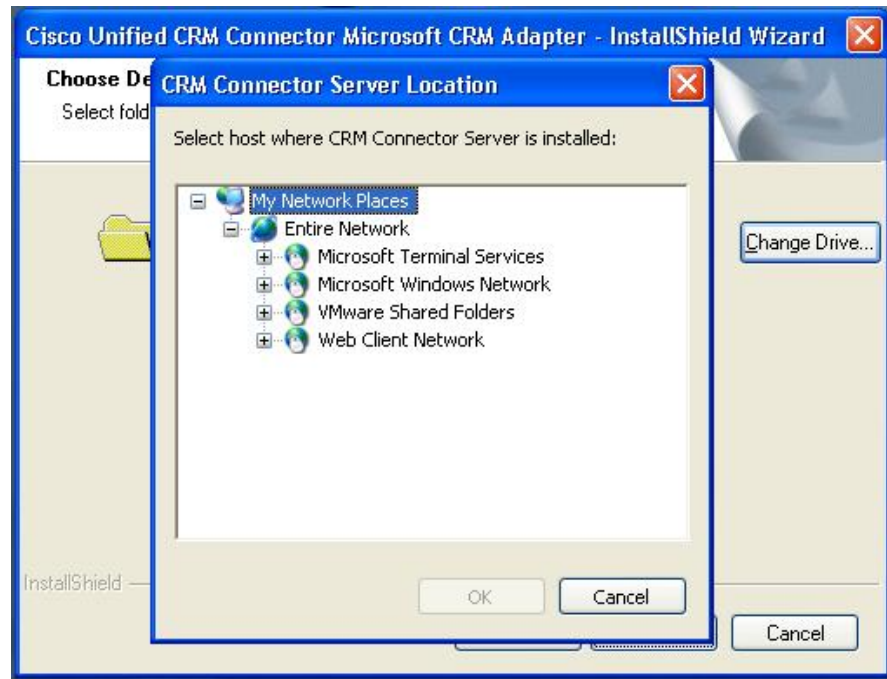
- Use the drop down to select a local system drive on which to install the adapter. Press OK to complete the selection and return to the “Choose Destination Location” dialog.

Note, this dropdown will only list physical drives, it will not display mapped network drives.

- Press Next to continue the installation.

Step 3: Identify the Cisco CRM Connector Server.

- You must now configure the location of the Cisco CRM Connector Server. Use the navigation tree to select the server where the CRM Connector Server is installed. Press “OK” to continue the installation.



Step 4: Enter Microsoft CRM credentials.

- Next you are prompted to enter the Microsoft CRM System Administrator credentials. You must specify a domain user account.
 - Enter or browse for the user name. You must specify the Windows domain as well as the user account name. Use a slash to separate the domain name from the user name.
 - Enter the password. Enter the user password.
- Press Next to continue the installation.

Cisco Unified CRM Connector Microsoft CRM Adapter - InstallShield Wizard

Microsoft CRM 3.0 Administrator Credentials

Specify user name and password for Microsoft CRM System Administrator account. If you are not sure about the credentials, abort installation now - it will not be functional anyway!

The name must be in DOMAIN\username format.

User name:

Password:

Select the button below to specify information about a new user that will be created during the installation.

New User Information...

InstallShield

< Back Next > Cancel

Step 4A: Use the Browse button option

- You may browse for the user credentials, pressing the browse button opens a dialog.
- The browse buttons on this dialog allow you independently to select the domain and user name (or you may hand-enter the domain and user name in the appropriate text box).

Step 5: Specify database location and user credentials.

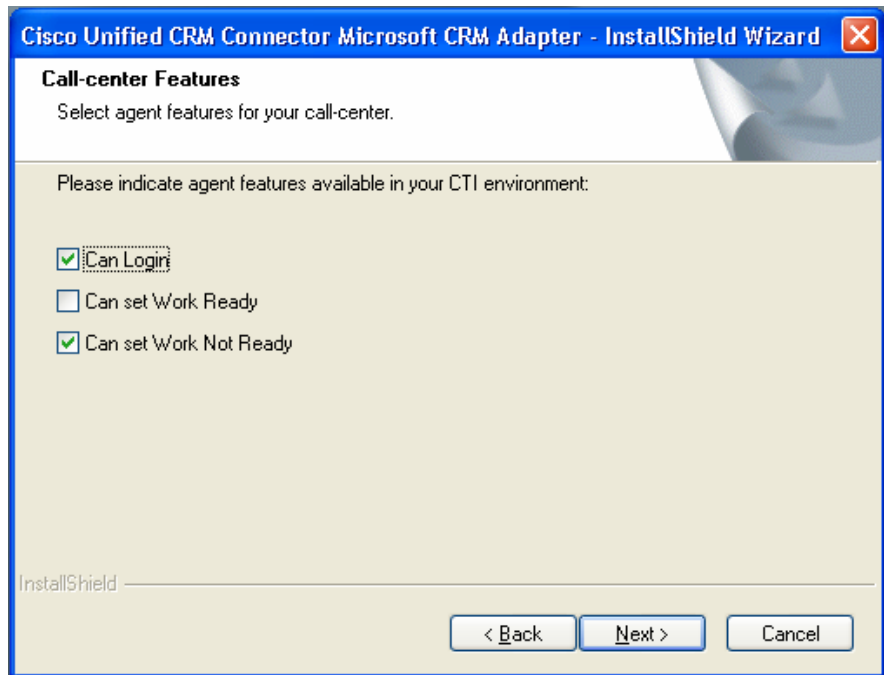
- Specify the location of the Microsoft CRM database and the user credentials to create and own the Cisco CRM Adapter schema elements. These credentials also are used by the web services to access the database.

The screenshot shows a Windows-style dialog box titled "Cisco Unified CRM Connector Microsoft CRM Adapter - InstallShield Wizard". The main heading is "Microsoft CRM Database Server". Below this, it says "Select Microsoft CRM 3.0 database server and specify connection credentials." and "Select the database server to install to from the list below or click Browse to see a list of all database servers." There is a "Database Server:" label followed by a text box containing "(local)" and a dropdown arrow, and a "Browse..." button. Below that, it says "Connect using:" followed by a radio button selected for "SQL Server authentication using the Login ID and password below". There are two text boxes: "Login ID:" containing "sa" and "Password:" containing masked characters. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The "InstallShield" logo is visible in the bottom left corner of the dialog area.

- Use the drop down to discover and select the SQL Server database instance (or you may browse for the database).
- Enter the SQL Server authentication credentials: login and password. Press Next.

Step 6: Configure the supported channel functions.

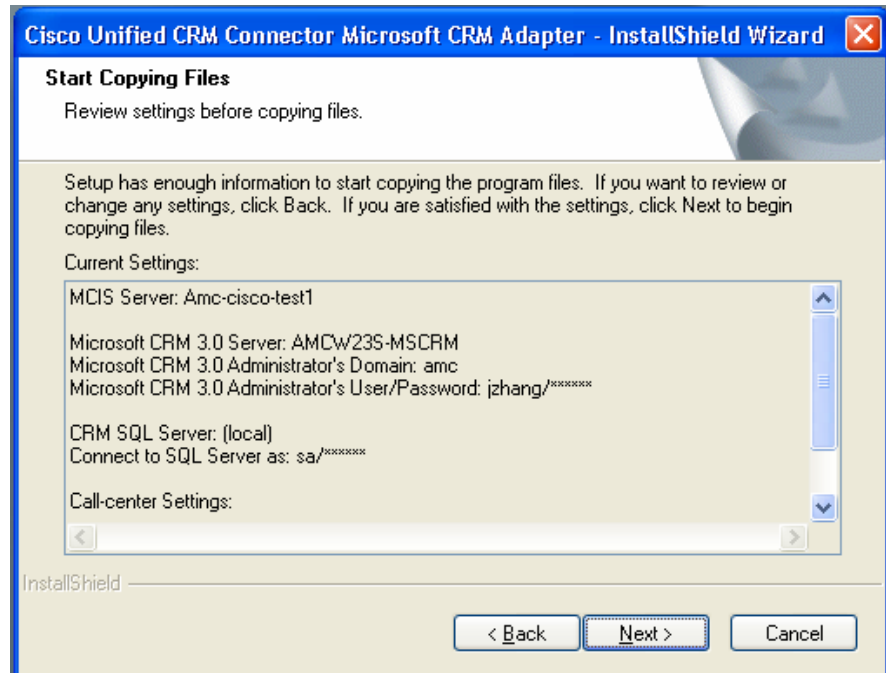
- You must specify the supported call center features. This identifies the supported ACD work states. Not all PBXs can support all work modes. Also, you may choose to limit these options if your call center procedures require agents to login into the telephone set or otherwise restricts these features.



- Use the checkbox to select the features supported CTI services and that you wish to enable for your software control.
 - **Can Login** – this enables login through the adapter and the Cisco Contact Center controller.
 - **Can Set Work Ready** – enables the “Set Work Ready” feature on the Cisco Contact Center controller. Work Ready leaves agents available for queued calls while performing other work.
 - **Can set Work Not Ready** – enables the “Set Work Not Ready” features on the Cisco Contact Center controller. Work Not Ready sets an agent unavailable for queued calls while performing other work.
- **Press Next to continue the installation.**

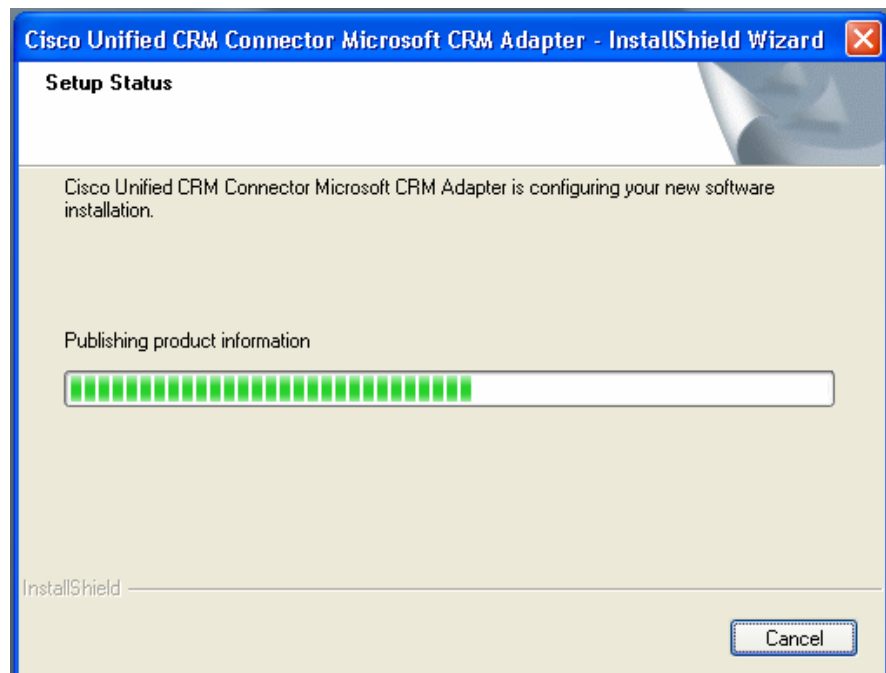
Step 7 Review installation criteria and install the adapter.

- Review the installation criteria; scroll down to check the Call-Center Settings.
- Press Next.

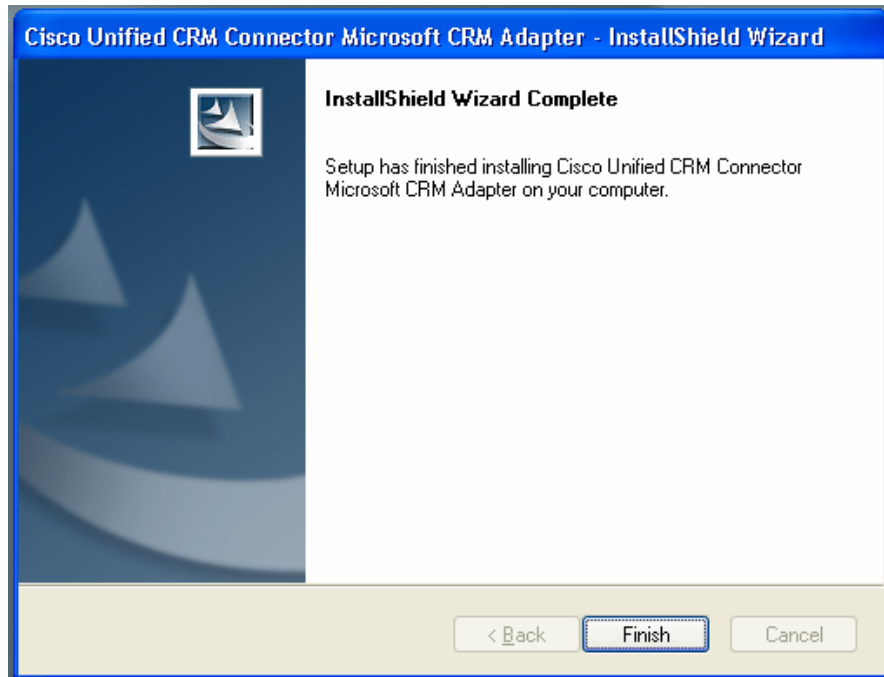


Step 8 Install files and complete installation.

- The installer will now copy the adapter files, install the adapter and create the data schema. A progress bar tracks the installation process.



- After installing the adapter files and database schema the Wizard launches a command prompt that runs an MS CRM customization script.
- When the installation is complete you are informed and prompted to press Finish to complete the install.



- Press **Finish** to close the Installation Wizard. Then close the Cisco Installation menu.

Table 9-2: Cisco Adapter for Microsoft CRM 3.0 Directory Structure shows the key installation directory structure and the files installed.

Table 9-2: Cisco Adapter for Microsoft CRM 3.0 Directory Structure

| Sub-Directory | Component | Use |
|---|---|---|
| C:\Program Files\Cisco\CRM Connector | | This is the parent drive location; all agent desktop application adapters will be installed under this directory hierarchy. |
| C:\Program Files\Cisco\CRM Connector\MS CRM Adapter | | This is the Microsoft CRM Adapter install directory. It and its subdirectories hold all of the application files and the configuration files. |
| | amcCC.aspx amc_mscrm.js amc_snlibs.js | These are web pages and Java scripts that support the Cisco Contact Center addition to the Microsoft CRM application. |

| Sub-Directory | Component | Use |
|---|--|---|
| | PrecompiledApp.config web.config | These are web services configuration files. Web configuration files are XML files that identify resources and configurations used to access web services. The web.config file in this directory holds the URL to access CRM Connector web services. It also specifies the credentials the web services use to access the Microsoft CRM Adapter's schema. |
| C:\Program Files\Cisco\CRM Connector\Application Adapter\AMC_Settings | | This directory holds web configuration settings, web pages and images used by the Cisco Contact Center add-in. |
| | 16_alert.gif Default.aspx Error.htm phone.aspx phonemod.aspx popup.aspx queuemod.aspx reason.aspx reasonmod.aspx template.css | These are web page elements and images of the Cisco Contact Center add-in. |
| | Web.config PrecompiledApp.config | These are web configuration XML files The web.config file in this directory identifies the MS CRM schema access credentials and the location of MS CRM services (URL). |
| C:\Program Files\Cisco\CRM Connector\Application Adapter\Logs | | The default logs directory. |

Configuring the CRM Adapter for Microsoft CRM 3.0

Quick Summary

The CRM Adapter for Microsoft CRM 3.0 uses the .Net Adapter Soap web services. These are installed on the CRM Connector server's IIS server.

Configuring Web Services Components

Web services are configured using **web.config** files, XML files found in application directories. The Microsoft CRM Adapter has two web.config files, as listed in Table 9-2: Cisco Adapter for Microsoft CRM 3.0 Directory Structure. These configure the URLs used to access the CRM Connector web services, adapter operational settings, such as trace levels, and database connection credentials used when web services access and update the adapter's database information.

Each web.config file has a <Configuration> section that is divided into three sub-sections: <AppSettings>, <connectionStrings> and <system.web>.

- **<AppSettings>** -- this configures web services URLs and operational settings.
- **<connectionStrings>** -- this configures the database connection methods and credentials for database access.
- **<system.web>** -- this configures system behaviors and authentication methods for ASP.NET. You will not change the system.web configuration settings.

The XML you will be configuring are clearly labeled as key / value pairs. The key name prefixed by the keyword “key=” and the value by the keyword “value=”. The key value pairs are on a single line delimited by angle brackets. This is an example key / value pair.

```
<add key="TraceLevel" value="DEBUG" />
```

Configure the parameter by changing the “value” element.

Warning: When editing an XML file only change the “value” information. Do not change keys or settings or other parameter names. Also be careful not to change the XML formatting. **Always backup configuration files before editing them.**

Configuring Settings in the Cisco Contact Center

In addition to configuring web services access settings, you must use the CRM Adapter for Microsoft CRM 3.0 administration tools to configure global and agent specific adapter settings. These are part of the Cisco Contact Center add in and are accessed through the Microsoft CRM application.

Additional Customizations

Finally, you may customize certain components of the Cisco Contact Center user interface, such as the “home web page,” using Microsoft CRM 3.0 customization tools

Configure Web Service Access

The web service application settings associate each named web service with a URL used to access it. These are set in the <AppSettings> section of the web.config file located in the C:\Program Files\Cisco\CRM Connector\Application Adapter.

In most cases these are properly configured by the adapter installation program. However, if your implementation uses a non-standard port for accessing the web services (other than port 80 or port 8080) as configured in the IIS service), you will need to specify the access port in the URL. Also, if you ever move the CRM Connector Server or wish to associate the Microsoft CRM Adapter implementation with another CRM Connector Server, you will need to change these settings.

Error! Reference source not found. shows the full web.config file. The yellow highlight <appSettings> section configures two different application settings types:

- The web services location settings. These have a “key” of the web service name and a value of the web service URL. **Table 9-3: Web Service URL Settings Entries** lists these URL values. You should only change the host name section of this URL to point to the IIS server running CRM Connector web services and the service port.
- Operational settings. These keys configure adapter behavior and are described in **Table 9-4: Adapter Operational Configuration Parameters**.

Table 9-3: Web Service URL Settings Entries

| |
|---|
| <value>http://hostname/AMCDoNetAdapterWebService/ContactAssociatedDataManagement.asmx</value> |
| <value>http:// hostname /AMCDoNetAdapterWebService/ContactManagement.asmx</value> |
| value>http:// hostname /AMCDoNetAdapterWebService/TelephonyServices.asmx</value> |
| <value>http:// hostname/AMCDoNetAdapterWebService/WorkTopManagement.asmx</value> |
| <value>http:// hostname /AMCDoNetEventAdapterWebService/AMCEventService.asmx</value> |

Table 9-4: Adapter Operational Configuration Parameters

| XML key / value entry | Valid values / Default | Meaning / Use |
|---|---|---|
| Application Adapter Channel Configuration Settings | | |
| <add key="DataStore" value="DataStore" /> | DataStore | The data store configured for the CTIModule. Default=DataStore |
| <add key="EventTimeout" value="5" /> | Positive integer value Default=5 | The event response timeout in seconds. |
| <add key="TraceLevel" value="DEBUG" /> | ERRORS WARNINGS INFO DEBUG Default=DEBUG | This sets the trace level for log files. |
| <add key="DefaultLoggedInState" value="NOT_READY" /> | READY NOT_READY WORK_READY WORK_NOT_READY Default=NOT_READY | This sets the agent work state when the toolbar logs in the agent ACD. |
| <add key="CanLogin" value="Y" /> | Y N Default=Y | CTI service supports ACD login. |
| <add key="CanSetWorkReady" value="N" /> | Y N Default=N | The user can log into the ACD and set ready for work. Note: this is ignored and treated as “NO” if “CanLogin” is NO. |

| | | |
|---|---------------------|---|
| <code><add key="CanSetWorkNotReady" value="Y" /></code> | Y N Default=Y | The CTI Services can set the agent work ready. Most ACDs can support this. |
| <code><add key="CanDeflect" value="N" /></code> | Y N Default=N | This allows agents to “deflect” inbound calls they are not prepared to answer. If enabled, the “Deflect” button is enabled when an inbound call alerts (rings) on the agent’s phone. |
| <code><add key="CanBTransfer" value="Y" /></code> | Y N Default=Y | Allows agents to execute blind transfers. Some call centers choose to disable this feature, allowing agents only to execute warm transfers, with a consultative call. |
| <code><add key="LogDir" value="C:\Cisco\CRM Connector\Application Adapter\LOGS" /></code> | A valid directory. | This is the location of the adapter log files. This can be any valid location, including a network directory. The default is listed in the value section of the key-value pair. |

The connection settings are highlighted in turquoise. These provide the database access credentials.

```
<add name="AMCT_MSCRM_ConnStr"
    connectionString="Data Source=(local);Initial
Catalog=AMCT;User ID=sa;Password='ciscocisco' "
    providerName="System.Data.SqlClient" />
```

This is a configuration parameter, rather than a key-value pair. It adds the named connection string “AMCT_MSCRM_ConnStr” with two parameters, the connectionString parameter and the providerName parameter.

- **Name:** This is the connection string name: do not change this value.
- **connectionString:** These specify the data source, the default SQL server schema (catalog) and the user credentials for accessing the database.
 - Data Source – this is the name of the SQL Server instance. If you need to change the instance, you can do that by modifying this data source entry.
 - Catalog – this is the Cisco adapter’s data schema name, do not change this setting.
 - User ID – this is the user name used to access the database.
 - Password – this is the password used to access the database.

- **providerName** – this identifies the database access client; do not change this value.

Example 9-1: Web Config File from Microsoft Adapter directory

```
<?xml version="1.0"?>
<!--
    Note: As an alternative to hand editing this file you can use the
    web admin tool to configure settings for your application. Use
    the Website->ASP.NET Configuration option in Visual Studio.
    A full list of settings and comments can be found in
    machine.config.comments usually located in
    \Windows\Microsoft.Net\Framework\v2.x\Config
-->
<configuration xmlns="http://schemas.microsoft.com/.NetConfiguration/v2.0">
    <appSettings>
        <add key="crm30sdk.crmService" value="http://Cisco23S-
MSCRM/mscrmservices/2006/crmService.asmx" />
        <add key="amcWorkTopManagement.WorkTopManagement"
value="http://Icmaw/AMCDotNetAdapterWebService/WorkTopManagement.asmx" />
        <add key="amcContactManagement.ContactManagement"
value="http://Icmaw/AMCDotNetAdapterWebService/ContactManagement.asmx" />
        <add key="amcTelephonyServices.TelephonyServices"
value="http://Icmaw/AMCDotNetAdapterWebService/TelephonyServices.asmx" />
        <add key="amcCADManagement.ContactAssociatedDataManagement"
value="http://Icmaw/AMCDotNetAdapterWebService/ContactAssociatedDataManagement
.asmx" />
        <add key="amcEventService.AMCEventService"
value="http://Icmaw/AMCDotNetEventAdapterWebService/AMCEventService.asmx" />
        <add key="DataStore" value="DataStore" />
        <add key="EventTimeout" value="5" />
        <add key="TraceLevel" value="DEBUG" />
        <add key="LogDir" value="C:\Program Files\Cisco\CRM Connector\Application
Adapter\LOGS" />
        <add key="DefaultLoggedInState" value="NOT_READY" />
        <add key="CanLogin" value="Y" />
        <add key="CanSetWorkReady" value="Y" />
        <add key="CanSetWorkNotReady" value="Y" />
    </appSettings>
    <connectionStrings>
        <add name="AMCT_MSCRM_ConnStr"
connectionString="Data Source=(local);Initial Catalog=AMCT;User
ID=sa;Password='ciscocisco'"
providerName="System.Data.SqlClient" />
    </connectionStrings>
    <system.web>
        <compilation debug="true"/>
        <authentication mode="Windows"/>
        <identity impersonate="true"/>
        <customErrors mode="Off"/>
        <httpModules>
            <add type="System.Web.SessionState.SessionStateModule"
name="Session"/>
        </httpModules>
    </system.web>
</configuration>
```

```
</configuration>
```

Configure Cisco Contact Center web settings.

The Cisco Contact Center web.config file is in the AMC Settings subdirectory (see **Table 9-2: Cisco Adapter for Microsoft CRM 3.0 Directory Structure**).

This configures the application settings and connection string for the end-user session: the agent's or administrator's Cisco Contact Center session. There are two important settings highlighted in yellow in Example 9-2: Cisco Contact Center web.config Settings:

- **Connection Info:** This configures SQL Server access credentials for the end-user session. Use the same data source and user credentials as you did for the web services web.config connection string.
- **MSCRM Settings:** This configures the web pages for the Cisco Contact Center extensions: **DO NOT CHANGE THIS SETTING.**

Example 9-2: Cisco Contact Center web.config Settings

```
<?xml version="1.0"?>
<!--
    Note: As an alternative to hand editing this file you can use the
    web admin tool to configure settings for your application. Use
    the Website->ASP.NET Configuration option in Visual Studio.
    A full list of settings and comments can be found in
    machine.config.comments usually located in
    \Windows\Microsoft.Net\Framework\v2.x\Config
-->
<configuration>
  <appSettings>
    <!-- SQL settings key -->
    <add key="ConnectionInfo" value="Data Source=(local);User
ID=sa;Password=ciscocisco" />
    <!-- MSCRM settings key -->
    <add key="crmsdk.crmService" value="http://AMCW23S-
MSCRM/mscrmservices/2006/crmService.asmx" />
  </appSettings>
  <connectionStrings/>
  <system.web>
    <!--
      Set compilation debug="true" to insert debugging
      symbols into the compiled page. Because this
      affects performance, set this value to true only
      during development.
    -->
    <compilation debug="true">
    </compilation>
    <!--
      The <authentication> section enables configuration
      of the security authentication mode used by
      ASP.NET to identify an incoming user.
    -->
```

```

<authentication mode="Windows"/>
<!--
The <customErrors> section enables configuration
of what to do if/when an unhandled error occurs
during the execution of a request. Specifically,
it enables developers to configure html error pages
to be displayed in place of a error stack trace.

<customErrors mode="RemoteOnly"
defaultRedirect="GenericErrorPage.htm">
    <error statusCode="403" redirect="NoAccess.htm" />
    <error statusCode="404" redirect="FileNotFound.htm" />
</customErrors>
-->
<identity impersonate="true"/>
</system.web>
</configuration>

```

Configure Cisco Contact Center global and agent settings.

Follow the directions in the next section, administering the Cisco Contact Center, to configure global and agent settings. You will need to configure these global settings.

Cisco Contact Center Administration Overview

Introduction

This section describes the Cisco Contact Center administration process: how to configure global and agent specific settings.

The administration pages are part of the Cisco Contact Center, the adapter extension to Microsoft CRM. Many of the configuration settings have already been set to default values or been pre-configured for you as part of the install. You will be configuring two types of settings: global settings that apply to all users or resources that can be assigned to individual users, and agent settings that configure and assign resources to an individual agent.

Global settings include:

- ACD queues
- Reason codes (e.g., not ready reasons)
- Global “Favorites” quick dial contact numbers that can be accessed by all agents in the contact center.

Each agent needs to be assigned these agent-specific configuration settings:

- Screen pop search / launch criteria.
- An extension
- ACD login credentials: Cisco user name and password.

- Screen pop search criteria and order.
- ACD queue assignments, from the global settings.
- Chanel ID – this is the Channel ID for the Cisco CRM Connector CTI Module the agent is assigned. By default this will be set to CTI1.

In addition, agents will be able configure:

- Extension – this is configurable so that agents in centers that use hotelling (or “hot seating”) can over-ride their configured extensions.
- Personal “Favorites”– quick dial contact numbers. These will be integrated with the global settings.
- Recent Contact Size – this is the number of recent contacts to be kept in a quick history drop down.
- Auto Clear Mode – this determines whether the last transaction screen pop is cleared automatically when the agent goes ready for the next transaction or whether the agent must manually clear it.

Before you begin

You will need a Microsoft CRM account with administrative privileges.

Accessing the Administration Pages

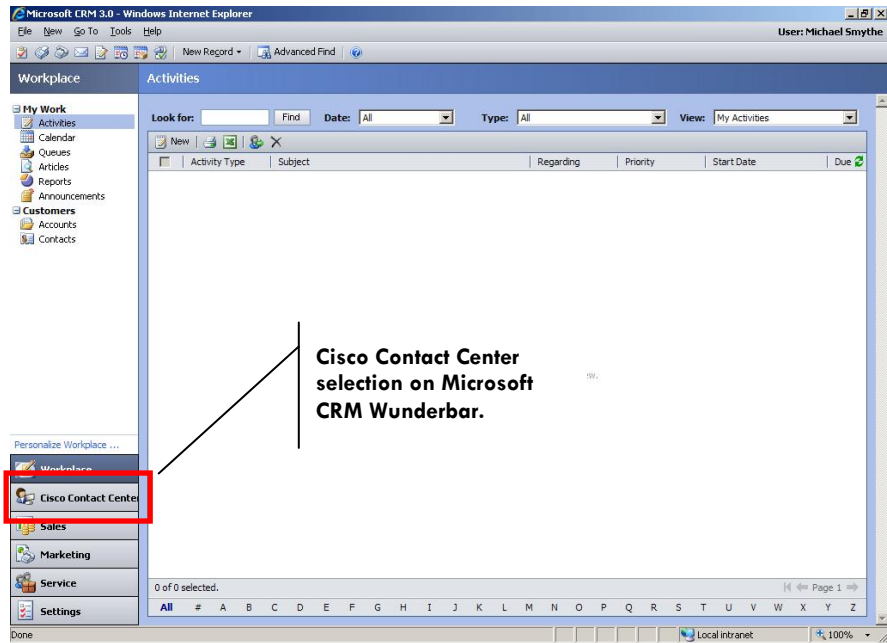
This section describes how to navigate to the Cisco Contact Center Administration Pages.

Step 1: Log into Microsoft CRM .

Log into Windows with a Microsoft CRM system administrator account.

Open an Internet Explorer browser session and connect with your Microsoft CRM application. This will open the Microsoft CRM Client. The Cisco Contact Center option is installed in the “Wunderbar.”

Figure 9-1: Microsoft CRM w/ Cisco Contact Center



Step 2: Select the Cisco Contact Center.

Select the Cisco Contact Center option, to open the Cisco Contact Center navigation tree “Home Page.” By default this is the Cisco web site. Change this to your web page using Microsoft CRM customization.

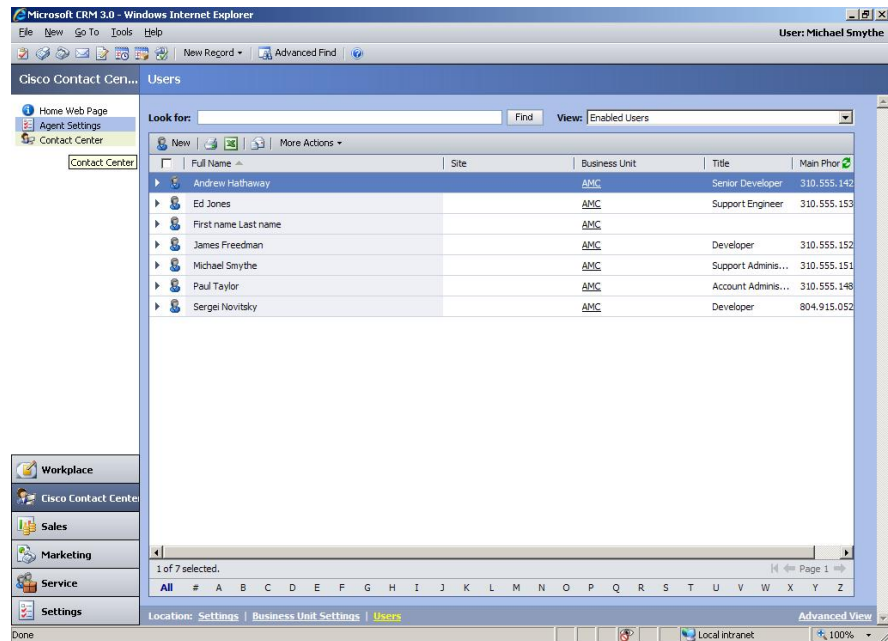
Figure 9-2: Cisco Contact Center Home Page



Step 3: Select “Agent Settings” from the Cisco Contact Center navigation tree.

This lists all MS CRM agents; select any agent to configure the global settings.

Figure 9-3: Cisco Contact Center Agent Settings Page



Select an agent account and double-click on the agent account or right-click and select “Open” from the pop-up menu. This opens a new “User” window

Figure 9-4: Agent User Window, General Tab

Step 4: Select the Cisco Contact Center tab.

The first two tabs, General and Address are standard Microsoft CRM agent information tabs. The third tab, Cisco Contact Center was added by the Adapter configures contact center.

Figure 9-5: User, Cisco Contact Center Tab

Figure 9-5: User, Cisco Contact Center Tab shows the Contact Center configuration options. This page is divided into two parts:

- Agent configuration settings at the top (Extension, Auto-Clear On Ready, Recent Contact Size and Favorites.) Administrators or agents may configure these settings.
- Admin Only. Only administrators may set these settings. They will be visible, but grayed out for agents.

You are now ready to configure global settings.

Configuring Global Settings.

Overview

Global settings establish default configurations for all agents or create resources that may be assigned to or used by any agent. The global settings are. This section identifies each global setting on the Cisco Contact Center, explains its use, how to configure it and how to assign it to an agent.

Global Settings include

- Favorites
- Reason Codes
- Queues

Favorites

Overview

Favorites are quick dial numbers that identify a contact target name and phone number. The contact target may be a customer, another agent, a supervisor or a queue DN.

Figure 9-6: Favorites Administration Settings



Administrators may create public Favorites that may be assigned to any agent. This is useful in for creating quick dials to reach supervisors and other agents, or key transfer queues for experts or to redirect calls.

Creating a Favorite.

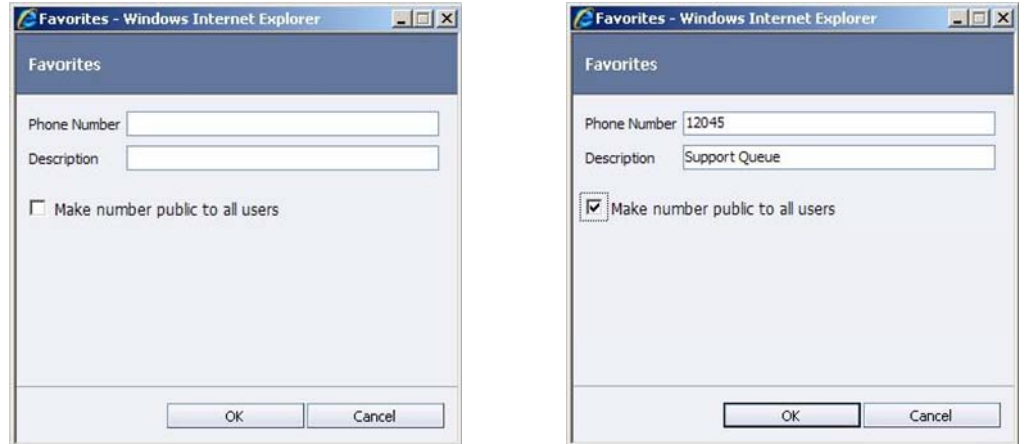
Use the “New” button to create a public Favorite.

This launches the “Favorites” dialog.

Enter the Phone Number and the Description. Check the “Make number public to all users” check box to create a public favorite. If this box is not checked, the Favorite will be assigned to the current agent only.

Press OK to save the Favorite, it will now appear in the Favorites drop down list.

Figure 9-7: Favorites Dialog



Editing a Favorite

You may edit the Favorite description, to correct or change the name. You may not edit the Phone Number.

Step 1: Select the Favorite in the drop down list.

Step 2: Press the Edit button. This opens the Favorites dialog for editing.



Step 3: Edit the Favorite description, then press OK to close and save the change or Cancel to abort and discard the change.

Deleting a Favorite

You may delete any favorite, whether public or agent specific.

Step 1: Select the Favorite from the drop down list.

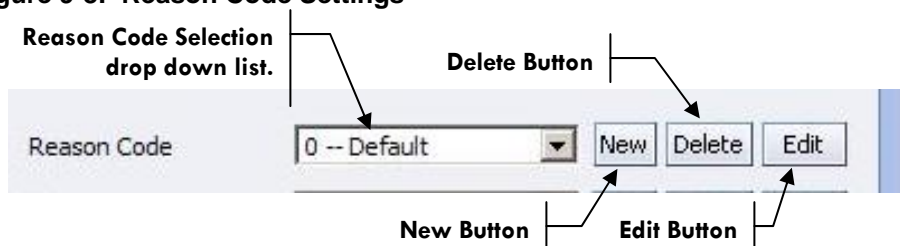
Step 2: Press Delete to delete the Favorite.

Reason Codes

Overview

Reason codes are used to associate reasons with when agents change their session status by going not ready to take a break or perform other work. There are two parts to reason codes, the “reason,” a text label and the reason number. The reason number is the same number assigned to the reason code in the ACD. By associating a text label “Description” with the reason code, agents do not need to memorize numeric reason codes.

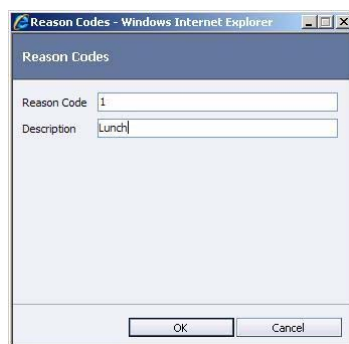
Figure 9-8: Reason Code Settings



Enable reason codes by defining them. If reason codes are enabled, agents must select a reason code before setting themselves not ready for other work or to take a break.

Create a Reason Code

Step 1: Press the New Button. This will open the Reason Code dialog.



Step 2: Enter the Reason Code. By default this will be the next higher sequential number. You may change the reason code to match the reason code configured within Cisco Contact Center or for the ACD.

Step 3: Enter the Reason Description. This is a display label agents will select when they are prompted to select a reason code.

Step 4: Press OK to save the new reason code, press cancel to discard without saving. This will close the Reason Code dialog.

Edit a Reason Code.

You may not change the reason code, but you may change the reason code description (label).

Step 1: Select the Reason Code from the drop down list. This opens the Reason Code dialog for editing.

Step 2: Change the Description (the reason code will be grayed out).

Step 3: Press OK to save the changes or Cancel to discard them. This will close the Reason Code dialog.

Delete a Reason Code

Deleting a reason code removes it from the list and makes the reason code number available again.

Step 1: Select the Reason Code from the drop down list.

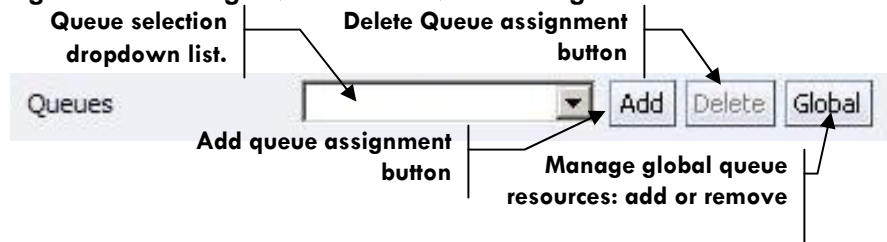
Step 2: Press the Delete button, this deletes the reason code.

Queues.

Overview

The Queues section manages queues. When agent log into ACDs they must associate themselves with queues so that the CTI services can monitor and set them available within one or more queues.

Figure 9-9: Manage Queues and Queue Assignment



Queues are global resources. You manage the queue as a global resource: you define it as an available queued resource or remove it from the list of available queues.

After defining a queue you may manage agent queue assignments by assigning the queue to agents or remove agent queue assignments. Agents may be assigned to one or more queues.

IMPORTANT WARNING: You must define at least one global queue in the Microsoft CRM configuration to assign to each agent, even if you do not use queues (or skills) in UCC or the ICM integrated ACD. You may assign a “phantom” queue value, such as 1, 10 or 9999. Agents will not be able to log in without a queue assignment.

Creating a Global Queue Resource

Creating a queue as a global resource makes it available for assignment to one or more agents.

Step 1: Click the “Global” button. This opens the global Queue Admin dialog.



Step 2: From the drop down, select “Add values to public queue” and press the Go button. This opens the Queue Admin, add number to public queue list dialog. This dialog shows all available global queues.



Step 3: Enter a queue number, press the Add button to add it to the global list.



Step 4: Press OK to close this dialog.

Step 5: Press OK on the Queue Admin dialog to close it.

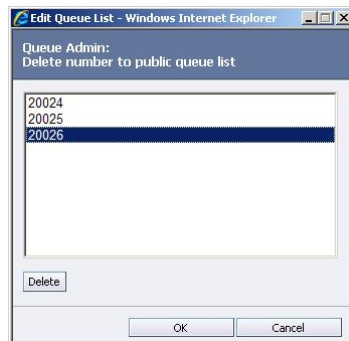
Remove a Global Queue Resource

This removes a queue from the list of available queues.

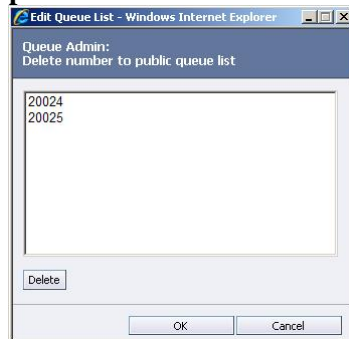
Warning: Removing a queue from the list does not remove it from existing agent assignments. If a queue is being deleted, you should remove it from all assigned agents and **then** remove it from the global list.

Step 1: Select the “Global” button. This opens the global Queue Admin dialog.

Step 2: From the drop down, select “Delete values from public queue.” This opens the Queue Admin: Delete number from public queue list dialog.



Step 3: Highlight the queue number to delete from the list. Then press Delete to remove the queue number.



Step 4: Press OK to close this dialog.

Step 5: Press OK on the Queue Admin dialog to close it.

Configuring Agent Specific Settings

Overview

Agent specific settings affect the configuration of a single agent. Individual agent settings include:


- Agent extension.
- Agent queue assignment
- Channel ID
- Agent ACD credentials (Agent ID and Password)
- Screen pop criteria and search sequence.
- Recent Contact Size
- Auto-Clear On Ready.

Note: To set an individual agent, you must open the agent's User dialog from the Cisco Contact Center Agent Settings page.

Note: Individual agent settings must be saved before the User dialog is closed. Press the **Save and Close** button on the menu bar or press the floppy disc drive icon on the menu bar or select **File->Save** from the drop down menu to save changes to agent settings.

Agent Extension

By default the agent extension is populated with the agent's number on the General settings tab.



The screenshot shows a window titled "CTI" with a tab labeled "Extension". Inside the window, there is a text box containing the number "310.555.1511". An arrow points from the text "Extension text box" to this text box.

Step 1: Enter the agent's assigned extension into the Extension text box. This entry should match your internal dial plan. Save the extension assignment when you close and save the agent's User dialog.

If your center does not assign agents extensions, if your center uses "hot seating," then you may leave this blank or with the default. Agents must be trained to enter the desk's extension before they start their daily session.

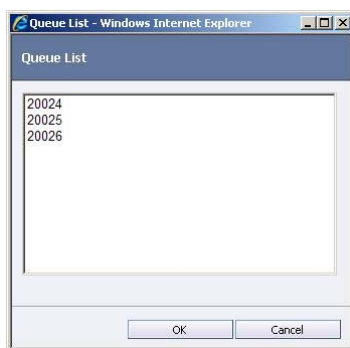
Queue Assignment

Assign a Queue to an Agent.

IMPORTANT WARNING: You must assign at least one queue to each agent, even if you do not use queues (or skills) in UCC or the ICM integrated ACD. You may assign a “phantom” queue value, such as 1, 10 or 9999. Agents will not be able to log in without this queue assignment.

Before assigning a queue to an agent you must create it as a global queue number.

Step 1: Select the “Add” button on the queue line. This opens the Queue List dialog that lists all available queues.



Step 2: Select a queue from the list.

Step 3: Press OK to assign the queue and close the dialog the queue is added to the agent’s queue list; or press Cancel to discard the assignment and close the dialog.

Step 4: Save the agent settings from the User dialog.

Remove Queue Assignment from Agent

This removes the queue assignment from only one agent.

Step 1: Select the queue to remove from the drop down list.

Step 2: Press the delete button. This removes the queue assignment from the current agent.

Step 3: Save the agent settings from the User dialog.

Channel ID Assignment

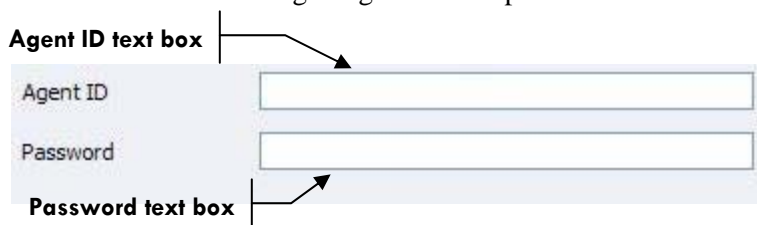
Each agent must be assigned to a configured CRM Connector channel. Use the Channel ID setting to associate the agent with the Cisco channel. The Channel ID **must match** one of the channel settings in the CRM Connector Server config.ini CTI module configurations.



To assign an agent to a channel, enter the Channel ID in the text box and save the agent’s User dialog settings.

Agent ACD Credentials

Each agent **must** have assigned ACD credentials; these are the ACD or Cisco Contact Center login Agent ID and password.

Agent ID text box | 

Agent ID

Password

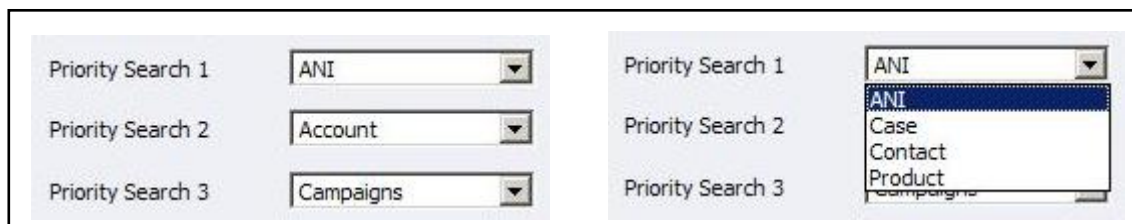
Password text box |

Enter the agent's ACD ID in the Agent ID text box and the password in the password text box.

Screen Pop Criteria and Search Order.

Overview

This determines which call data fields are used to launch the screen pop in the Cisco Contact Center. Screen pop populates the Contact Data section with customer information.



| Priority Search | Criteria |
|-------------------|-----------|
| Priority Search 1 | ANI |
| Priority Search 2 | Account |
| Priority Search 3 | Campaigns |

The left hand image shows the three priority search criteria, assigned values. The right hand drop down shows the other valid priority search criteria.

Screen Pop Value Types

Screen pop is based on known values in the call attached data. The Cisco Contact Center can execute a screen pop on these Microsoft CRM business object values. The values must be included in the call attached data to execute a screen pop. The Microsoft business object values are:

- ANI – “automatic number identification” this is the originating caller’s phone number. This is part of the standard call data attached to incoming calls. For outbound dials this is the number the agent dialed.
- Campaigns – this is a marketing campaign associated with “dialed number information service” (DNIS). This is based on the number the customer dialed to call into the company. DNIS is part of standard call data.
- Account – this is the customer account number. This is not part of standard call information, but it may be captured in the IVR and passed through the CRM Connector using ECC variables.

- Case – this is a support request or case number. This is not part of standard call information, but it may be captured and passed in ECC variables.
- Contact – this is the contact name or user identification. It differs from account, because account may be associated with two or more users, such as a corporate account. This is not part of standard call data, but it may be captured and passed through ECC variables.
- Product – this is a unique product ID. This is not part of standard call data, but it may be captured and passed through ECC variables.

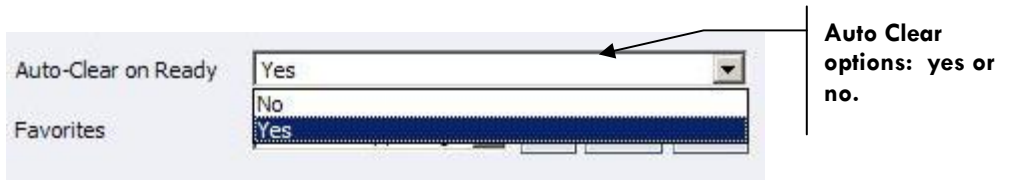
You may specify up to three screen pop criteria and prioritize the search order. The Cisco Contact Center will only perform a screen pop on one of the three criteria: the first priority to with a matching customer record.

Screen Pop Execution Process

When an inbound call is delivered to an agent, the Contact Center searches on the first priority search: here “ANI.” If no ANI match is found, it will then attempt to match on the second priority search value, “Account.”

If a match is found it will ignore the last priority search value, “Campaigns” and execute a screen pop; otherwise it will search for a matching campaign screen pop.

Set the Auto-Clear On Ready.



Use the drop down labeled “Auto-Clear On Ready” to configure this behavior. When enabled, this clears the last agent transaction screen pop when the agent is set ready on the ACD. If this is set to NO, then agents must clear this using the Clear button on the Contact Center page.

Set the Recent Contact Size.



The Recent Contact drop down is part of the Contact Controller. It lists recent contacts for the current session and their phone number. Agents place a call to a recent contact by selecting the record within the drop down.

The Recent Contact Size sets the maximum number of contacts in the drop down. The default is ten (10).