



ARI Deployment Guide for Cisco Unified Intelligent Contact Manager Enterprise & Hosted Editions

Release 7.2(1)

June 2007

Americas 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: 408 527-0833



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

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

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California. NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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, Packet, 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. (0705R)

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

Copyright © 2007 Cisco Systems, Inc. All rights reserved.

Table of Contents

Preface	1
Purpose	1
Audience	2
Organization	2
Related Documentation	2
Conventions.....	3
Obtaining Documentation.....	4
Cisco.com.....	4
Product Documentation DVD.....	4
Ordering Documentation.....	4
Documentation Feedback.....	5
Product Alerts and Field Notices	5
Cisco Product Security Overview.....	5
Reporting Security Problems in Cisco Products	6
Obtaining Technical Assistance.....	6
Cisco Technical Support & Documentation Website.....	7
Submitting a Service Request.....	7
Definitions of Service Request Severity.....	8
Obtaining Additional Publications and Information.....	8
1. About ARI Deployment.....	11
Supported ACDs in this Release of the ARI Deployment.....	12
Advantages of the ARI Deployment.....	12
Who Might Chose to Implement the ARI Deployment?.....	13
Supported Features.....	13
Unsupported Features.....	14
2. Architecture and Models for the ARI Deployment.....	15
Overview of Architecture and Core Components.....	15
Platform and Network.....	15
The Central Controller (Router and Logger).....	16
The Peripheral Gateway (PG).....	17
The ARS PG.....	18
The Admin Workstation (AW).....	20
The CTI Server.....	20
CTI OS.....	21
The ACD/PBX.....	21
The Voice Response Unit (VRU).....	21
Examples of Deployment Models for the ARI Solution.....	24
3. Installation and Configuration for the ARI Deployment.....	27
Installation.....	27
About the Server Where You Install ARS PG.....	27
Preparing a Server for the ARS PG.....	28
Installing the ARS PG on the Server.....	30
Installing CTI OS Server on the ARS PG Server Machine.....	35
Installing the Agent and IPCC Supervisor Desktops.....	36
Configuration.....	37
About ACD/PBX Configuration.....	38
About Configuration Manager.....	38

Configuring a Network VRU.....	39
Configuring Agent Desk Settings.....	40
Configuring the ARS PG.....	42
Configuring the ARS PG Peripheral: Peripheral Tab.....	43
Configuring the ARS PG Peripheral: Advanced Tab.....	45
Configuring the ARS PG Peripheral: Agent Distribution and Skill Group Mask Tabs.....	46
Configuring the ARS PG Peripheral: Routing Client Tab.....	46
Configuring the ARS PG Peripheral: Default Route Tab.....	47
Configuring the ARS PG Peripheral: Peripheral Monitor Tab.....	48
Configuring Agent Targeting Rules.....	49
Configuring for Reporting in an ARI Deployment.....	51
Notes on Other Configuration.....	52
4. Queuing, Routing, and Reporting with an ARI Deployment.....	57
Queuing.....	57
Routing.....	58
Device Targets and Agent Targeting Rules.....	59
Pre-Routing.....	60
Post Routing.....	60
Translation Routing.....	60
Scripting.....	61
Using WebView with your ARI Deployment.....	62
5. Desktops and Call Control.....	63
About Computer Telephony Integration.....	63
Agent Phones.....	63
Softphone.....	64
Hard Phones.....	64
Synchronization.....	65
Desktops and Call Control.....	65
The Agent Desktop.....	66
The Supervisor Desktop.....	66
Desktop Differences.....	67
Agent States.....	67
Changing Agent State from the Desktop.....	68
Notes on Agent State Transitions.....	68
Index	71

List of Figures

Figure 1: The ARS Gateway.....	20
Figure 2: External (Network) VRU.....	22
Figure 3: Virtual (embedded) VRU.....	23
Figure 4: ARS PG Added to Existing System.....	24
Figure 5: ARS PG Replaces TDM PG.....	25
Figure 6: New Deployment with all ARS PGs.....	25
Figure 7: Server for the ARS PG.....	28
Figure 8: Logical Controller ID.....	30
Figure 9: Peripheral ID.....	30
Figure 10: Setup: Select PG Component.....	31
Figure 11: Setup: Select ARS Client Type.....	31
Figure 12: Peripheral Gateway Component Properties.....	32
Figure 13: Setup: Add PIM popup.....	32
Figure 14: Setup: ARS PIM Configuration dialog box.....	33
Figure 15: Setup: Peripheral Gateway Component Properties.....	34
Figure 16: Setup: Device Management Protocol Properties.....	34
Figure 17: Setup: Peripheral Gateway Network Interfaces.....	35
Figure 18: Setup: Check Setup Information	35
Figure 19: CTI OS Peripheral Identifier Screen.....	36
Figure 20: Configuration Manager.....	39
Figure 21: Configuring Network VRU.....	40
Figure 22: Configuring Agent Desk Settings.....	42
Figure 23: Configuring the PG.....	43
Figure 24: Configuring the PG Peripheral.....	43
Figure 25: Configuring the PG Peripheral: Peripheral Tab.....	44
Figure 26: Configuring the PG Peripheral: Advanced Tab.....	45
Figure 27: Configuring the PG Peripheral: Agent Distribution Tab.....	46
Figure 28: Configuring the PG Peripheral: Routing Client Tab.....	47
Figure 29: Configuring the PG Peripheral: Default Route Tab.....	48
Figure 30: Configuring the PG Peripheral: Peripheral Monitor Tab.....	49
Figure 31: Configuring Agent Targeting Rules.....	51
Figure 32: Select the ARS PG when Configuring.....	52
Figure 33: Selection when Configuring Skill Groups.....	53

Figure 34: WebView Template Selection.....	62
--	----



Preface

Purpose

This guide provides information to help you understand, install, and configure the Agent Routing Interface (ARI) deployment.

The ARI deployment is supported for Cisco Unified Intelligent Contact Management Enterprise (Unified ICME) and Cisco Unified Intelligent Contact Management Hosted (Unified ICMH).

A note about new Cisco product names

- Cisco ICM Enterprise Edition is renamed Cisco Unified Intelligent Contact Management Enterprise (abbreviated as Unified ICME). Cisco ICM Hosted Edition is renamed Cisco Unified Intelligent Contact Management Hosted (abbreviated as Unified ICMH).
- Cisco IPCC Enterprise Edition and Cisco IPCC Hosted Edition are renamed Cisco Unified Contact Center Enterprise (abbreviated as Unified CCE) and Cisco Unified Contact Center Hosted (abbreviated as Unified CCH), respectively.
- Cisco CallManager is renamed Cisco Unified Communications Manager.

The new product names are being introduced in phases. In the 7.2(1) release, the new names refer to the product as a whole. They are not yet used for functions and utilities in the user interface. For example, the *ICM Admin Workstation* is not yet renamed and is still referred to as the *ICM* and not the *Unified ICM Admin Workstation*.

Although this guide refers to the product as a whole by its new name, it refers to components and utilities by the names that appear in the user interface.

Audience

This document is intended for anyone who plans to install, configure, and maintain an ARI deployment by adding an Agent Routing Service Peripheral Gateway (an ARS PG) to their Unified ICM Enterprise system.

Organization

In addition to this Preface, this guide contains five chapters and an index.

[Chapter 1 \(page 11\)](#) explains the concept and the advantages of an ARI deployment and lists supported and unsupported features.

[Chapter 2 \(page 15\)](#) gives an overview of the Unified ICM architecture and how an ARI deployment fits into that architecture.

[Chapter 3 \(page 27\)](#) covers installation for an ARI Deployment and what parameters to set for ARI in Configuration Manager.

[Chapter 4 \(page 57\)](#) discusses Queuing, Routing, and Reporting with an ARI Deployment.

[Chapter 5 \(page 63\)](#) explains agent and supervisor desktops and call control.

Related Documentation

CTI OS Agent Desktop User Guide for Cisco Unified ICM/CC Enterprise & Hosted

CTI OS Developer's Guide

CTI OS Supervisor Desktop User Guide

ICM Installation Guide for Cisco ICM Enterprise Edition

Hardware and System Software Specification (Bill of Materials) [located on cisco.com](http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html) (http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_user_guide_list.html)

Installation Guide Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.2(1)

IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition

Reporting Guide for Cisco Unified ICM Enterprise & Hosted

Reporting Guide for Cisco IPCC Enterprise & Hosted Editions

Staging Guide for Cisco ICM/IPCC Enterprise & Hosted Editions

System Manager Guide Supplement for Avaya ARS PG

Conventions

This manual uses the following conventions:

Convention	Description
boldface font	<p>Boldface font is used to indicate commands, such as user entries, keys, buttons, and folder and submenu names. For example:</p> <ul style="list-style-type: none"> • Choose Edit > Find. • Click Finish.
<i>italic font</i>	<p>Italic font is used to indicate the following:</p> <ul style="list-style-type: none"> • To introduce a new term. Example: A <i>skill group</i> is a collection of agents who share similar skills. • For emphasis. Example: <i>Do not</i> use the numerical naming convention. • A syntax value that the user must replace. Example: IF (<i>condition, true-value, false-value</i>) • A book title. Example: See the <i>Cisco CRS Installation Guide</i>.
window font	<p>Window font, such as Courier, is used for the following:</p> <ul style="list-style-type: none"> • Text as it appears in code or that the window displays. Example: <code><html><title>Cisco Systems, Inc. </title></html></code>
< >	<p>Angle brackets are used to indicate the following:</p> <ul style="list-style-type: none"> • For arguments where the context does not allow italic, such as ASCII output. • A character string that the user enters but that does not appear on the window such as a password.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL::

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at **tech-doc-store-mkpl@external.cisco.com** or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems Attn: Customer Document Ordering 170 West Tasman Drive San Jose, CA
95134-9883

We appreciate your comments.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can register to receive Cisco Product Alerts and Cisco Field Notices by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information. Access the tool at this URL: <http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en>.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only: security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies: psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Note: We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Note: Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pastingshow command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly

To open a service request by telephone, use one of the following numbers:

- Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
- EMEA: +32 2 704 55 55
- USA: 1 800 553-2447

Obtaining Additional Publications and Information

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1) - Your network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2) - Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3) - Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4) - You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

<http://www.cisco.com/go/guide>

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

<http://www.cisco.com/go/marketplace/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends,

technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

<http://www.cisco.com/ipj>

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

<http://www.cisco.com/discuss/networking>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



Chapter 1

About ARI Deployment

Agent Routing Integration (ARI) deployment allows the Unified ICM software to select agents and to route calls directly to them.

ARI is implemented by using an [ARS PG \(page 18\)](#).

Before ARI was introduced, the method by which Unified ICM interfaced with an Automatic Call Distributor (ACD) was through a customized TDM PG designed specifically for that ACD. Reporting management, agent skill mapping, and routing decisions remained under control of the ACD. It was the role of the ACD (and *not* Unified ICM), to select the agent. Although using TDM-specific PGs remains a viable deployment, the option of using an ARS PG adds flexibility to the Unified ICM environment.

In an ARI deployment with an ARS PG, traditional "ACD functions" move to the Unified ICM. The role of the ACD changes from a *TDM ACD* to an *ACD/PBX* that serves as the telephone switching system. In this role, the ACD/PBX provides connections for agent phones and connects a call to an agent, as directed by the Unified ICM Router.

As part of Unified ICM, the ARI deployment can be implemented in a single-site environment or integrated into a multisite contact-center enterprise.

In this guide, the term *ARI deployment* refers to Unified ICME systems where one or more ARS PGs have been added to, or have replaced, one or more TDM PGs. An ARI deployment might also be a Unified ICME system that uses ARS PGs only.

This section contains the following topics:

- [Supported ACDs in this Release of the ARI Deployment, page 12](#)
- [Advantages of the ARI Deployment, page 12](#)
- [Who Might Chose to Implement the ARI Deployment?, page 13](#)
- [Supported Features, page 13](#)
- [Unsupported Features, page 14](#)

Supported ACDs in this Release of the ARI Deployment

Each ARS PG supports only one ACD/PBX peripheral.

The ACD/PBX supported in Release 7.2(1) is the Avaya Communications Manager 3.0 or 3.1.2 with AES Server.¹

Advantages of the ARI Deployment

These are some advantages of deploying ARI with an ARS PG:

- **Call queuing** is controlled by Service Control Interface (SCI)-managed queue points. This is the case whether the VRU is at the network level or is premise-based on the ACD/PBX.

Queuing thus occurs such that Unified ICM retains control of the call. This is a distinct advantage over traditional, ACD-controlled queuing. The call does not 'get stuck at' the ACD, and Unified ICM does not lose control of the call. The call remains available for enterprise routing depending on agent availability and collected information. See [Queuing \(page 57\)](#).

- **Intelligent call routing through a single platform** and the **ability to route a call to a specific agent**

Because the ARS PG hands control for routing to the Unified ICM, you can rely on a single routing platform. When the ICM connects to traditional TDM PGs, the call is routed to a skill group at the ACD, not directly to the agent. With an ARS PG, the ICM can route to an agent, by login ID or extension.

- **Improved, consolidated reporting**

You can use WebView's reporting categories to monitor contact center agent performance, customer experience, and operational effectiveness—rather than running some reports from the ACD (such as ACD agent reports) and running other reports from WebView. See [Using WebView with your ARI Deployment \(page 62\)](#).

- **Transition to an IP Call Center**

Introducing an ARS PG is an intermediate solution and a migration path to what can eventually become a full IP solution.

- **Retention of existing ACD Hardware**

If you already deploy an ACD that interfaces to Unified ICM by a TDM PG (for example, if you already have an Avaya Communications Manager 3.1.2), there is no need to remove

1) Former names for the Avaya Communications Manager were the Avaya DEFINTY, the G3, and the Avaya MultiVantage.

or replace the switch hardware. With the ARS PG, you can use existing hardware (the legacy ACD), and connect to it with an ARS PG rather than a TDM PG.

- **Additional supervisory features**

Connection with the ARS PG extends the functionality of the agent and supervisor desktops. For example, supervisor barge-in and intercept—formerly offered only in an Cisco Unified Contact Center (formerly named IPCC) environment—become available in Unified ICM. See [The Supervisor Desktop \(page 66\)](#).

Who Might Chose to Implement the ARI Deployment?

Possible implementation scenarios include:

- Unified ICME customers who have legacy TDM PG connections to ACDs in place and who want to *add* an ARS PG and a [supported ACD/PBX \(page 12\)](#) to their deployment.
- Unified ICME customers who choose to *replace* their current TDM PG with the ARS PG, in effect handing control over to ICM and 'dumbing down' the ACD so that it serves as an ACD/PBX.
- New Unified ICME customers who plan to interface with ARS PGs only, rather than with TDM PGs.

See also [Examples of Deployment Models for the ARI Solution \(page 24\)](#)

Supported Features

These features are supported for the ARI solution:

- » Agent Reskilling by supervisors
- » Ability to allow mutually exclusive or concurrent use of hard phones and Cisco softphones
- » Ability to implement and configure [Agent Targeting Rules \(page 49\)](#)
- » Cradle-to-grave tracking (the ability to track a call from start to finish, independent of transfers, overflows, or diversions that occur during the life of the call)
- » Duplexing, for a fully redundant and fault-tolerant solution
- » Interactive voice response (IVR) integration
- » Interfaces for CTI-type integrations (includes third-party call control)
- » Monitoring of agent states

Unsupported Features

- » Monitoring of call data and call states
- » Pre-routing, post-routing, and translation routing
- » Reporting (a full set of ACD reports, including Agent-level reporting)
- » Scalability, as tied to the capacity for CTI OS servers that co-reside with Agent PG servers for IPCC Enterprise, New Deployments/Technology Refresh. See the *Hardware and System Software Specification (Bill of Materials)*. [Click here for the link to this document. \(page 2\)](#)
- » Supervisory barge-in and intercept functions
- » Unified ICM based routing for agents connected to the ACD/PBX

Unsupported Features

These features are not currently supported for ARI:

- » ACD Queues
- » Agent Desk Settings for AutoRecord on Emergency
- » Agent Desk Settings for Outbound Access
- » Blended Collaboration (multi-media integration)
- » Call recording
- » Call rerouting based on non-answer (RONA)
- » ICM Universal Queue
- » Manual entry of hardphone access codes
- » Outbound Option
- » Peripheral Service Level reporting
- » Remote Agent, Mobile Agent
- » Silent Monitoring on the CTI OS Supervisor desktop
- » Sub-skill groups
- » Service Bureau Configuration with shared resources
- » Trunk and Trunk Group reporting



Chapter 2

Architecture and Models for the ARI Deployment

This section contains the following topics:

- [Overview of Architecture and Core Components, page 15](#)
- [Examples of Deployment Models for the ARI Solution, page 24](#)

Overview of Architecture and Core Components

What follows is a summary of the components that comprise a Unified ICM system, noting how they do—or do not—differ for an ARI deployment.

For details on these components, refer to the *Preinstallation Planning Guide for Cisco ICM Enterprise Edition* and the *ICM Installation Guide for Cisco ICM Enterprise Edition*.

Platform and Network

The operating system, domain requirement, network interface, server platforms, and fault tolerance are described in the topic that follows.

Operating System

Unified ICM requires a Microsoft Windows operating system. Refer to the [Hardware and System Software Specification \(Bill of Materials\) \(page 2\)](#) for Operating System requirements.

Active Directory

Unified ICM software uses Windows Active Directory to control users' access rights to perform setup, configuration, and reporting tasks.

Overview of Architecture and Core Components

You can install Unified ICM software in an existing Windows domain (including the corporate domain) and control access to ICM functions using the Active Directory functionality your network already supports.

You must have added the Cisco Root Organizational Unit and at least one Facility Organizational Unit with one Instance Organizational Unit.

See the *Staging Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for details on Active Directory configuration and other network configuration requirements.

Network Interface

The ACD/PBX is typically connected to the telephone network by T1 or E1 lines.

Carrier networks offer services to deliver the following information about an incoming call by means of an intelligent incoming trunk (for example, Primary Rate Interface):

- Calling Line ID (CLID),
- Directory Number Identification Service (DNIS),
- Called Number
- Automatic Number ID (ANI).

Server Platforms

Unified ICM components (including the ARS PG Server) are supported only on Cisco MCS or MCS-equivalent servers.

See the [Hardware and System Software Specification \(Bill of Materials\) \(page 2\)](#) for further specifics on hardware requirements, including recommended platform sizing guidelines based on the types of available hardware systems.

Fault Tolerance

Fault tolerance for the ARS PG is no different than for other PGs. Side A is controlled by the Side A ARS PG. Side B is controlled by the Side B ARS PG.

Only one side is active at a time. If the Active side PG becomes inactive, both the PIM and ARS gateway of that side become inactive. Upon failover, the PIM and ARS gateway on the hot Standby side become the active side.

The Central Controller (Router and Logger)

The Central Controller serves as the clearinghouse for routing and reporting data—by receiving route requests, making routing decisions, and monitoring data messages about what is happening in the system.

The Central Controller is installed on one or more servers and comprises three major components: the CallRouter (Router), the Logger, and the Central Database.

- **CallRouter (Router)**

The **Router** receives notification from a Routing Client, such as a Network Interface Controller or a [Peripheral Gateways \(PGs\) \(page 17\)](#), that a call is in need of some form of routing. It then executes a user-defined script that specifies how the Routing Client is to handle the call.

The Router also receives messages from the PGs about agent and system status events in the network. Awareness of the current status of these resources is essential to the routing scripts.

The Router immediately forwards this data directly to the Admin Workstations so that it is available to appear in reports. The Router also writes records to the Central Database on the Logger.

- **Logger and Central Database**

The **Logger** receives data from the Router (such as detail messages about calls and summary messages that have been computed by the Peripheral Gateways) and serves as the interface between the Router and the SQL Server database manager.

The **Central Database** serves as a buffer where data is committed to quickly support the performance of the Router. The Central Database stores configuration data, as entered and changed on the Admin Workstation; routing scripts, also as entered and changed on the Admin Workstation; summary historical data passed from the Router; and call detail data.

FOR AN ARI DEPLOYMENT, the role of the Central Controller remains exactly as for a traditional Unified ICME environment.

The Peripheral Gateway (PG)

A *peripheral* is a device—such as an ACD—that receives calls that have been routed by the Unified ICM Central Controller.

Agents are grouped by peripheral for reporting, call handling, and other administrative purposes.

A *Peripheral Gateway (PG)* is a monitoring node through which the Unified ICM Central Controller communicates directly with a peripheral. The PG monitors status information from the peripheral and forwards that information to the Central Controller. The PG sends routing requests to the Central Controller and receives routing information in return. The term *PG* refers to both a physical hardware platform (server) and the logical software processes that run on it.

Unified ICM software has unique PGs for each device it supports, including switch-specific TDM PGs that connect to ACDs. For example, the Aspect PG and the Alcatel 4400 PG connect to an Aspect and Alcatel 4400 ACD, respectively.

A PG operates through the interaction of several processes, including:

- The **Peripheral Interface Manager (PIM)**, which manages communication between the PG and the peripherals. The PIM's main function is to convert peripheral-specific events and requests to an ICM-compatible peripheral data stream. Specifically, the PIM supplies the Open Peripheral Controller (OPC) with CSTA call event reporting messages. These messages form the basis of ICM real-time monitoring and historical reporting. The OPC process receives the CSTA messages from the PIM and uses them to construct the actual ICM real-time and historical routing and reporting data. (OPC is described in one of the following sections.)
- The **Open Peripheral Controller (OPC)**, which is the process that takes real-time data and events from the PIM and presents these data to the CallRouter. The OPC process forms the database objects the CallRouter needs to route calls and monitor real-time activity on the peripheral.

FOR AN ARI DEPLOYMENT, the role of the PG is modified for the ARS PG, as explained in the topic that follows.

The ARS PG

The ARS PG must be installed on a separate, dedicated server, co-located with CTI Server and CTI OS. See also [About the ARS PG Server Machine \(page 27\)](#).

A Unified ICM system can support an ARS PG plus *one or more* of the following:

- TDM PG
- Generic PG
- IPCC Gateway PG
- VRU PG
- ARS PG²

Processes on the ARS PG are described below.

PIM

With the ARS PG, the role of the **PIM** changes as follows:

- to perform the following operations: dial plan address translation, telephony device reporting, telephony device call control, and agent state transition validation.
- to receive new configuration objects, such as for DeviceTargets and AgentDeskTopSettings, as well as an updated version of the agent object.
- to validate agent state transitions.

2) Each ARS PG must be on a dedicated server.

OPC

With the ARS PG, the role of the **OPC** is enhanced as follows:

- to include support for the Agent Routing Service peripheral type.
- to provide support for delivering calls and call context to agents on the ACD/PBX.
- to synchronize agent availability as seen on the ACD/PBX with the state used by the Unified ICM when routing calls.

ARS PG Gateway

A new process, the *ARS Gateway* (see the topic that follows), runs co-resident with the PIM and the OPC on the ARS PG.

The ARS Gateway

The ARS Gateway is the process that transfers the traditional ACD functions to the Unified ICM.

The ARS Gateway maintains the heartbeat and connection between the ARS PIM and the ACD/PBX.

It communicates with the ACD/PBX via the PBX's proprietary interface and *translates* (that is, acts as a protocol converter for) call control, call events, device monitoring, and call routing messages between the ARS PIM and the ACD/PBX.

Each ARS PG has a unique ARS Gateway specific to the proprietary protocol of the ACD/PBX.

In this release, the ARS PG solution supports an ARS Gateway to the Avaya Communications Manager 3.0 or 3.1.2 with AES Server. For the Avaya, the protocol is ASAI 3.0 (Adjunct Switch Application Interface).

- The ARS Gateway communicates with the ACD/PBX by the ACD/PBX's proprietary interface.

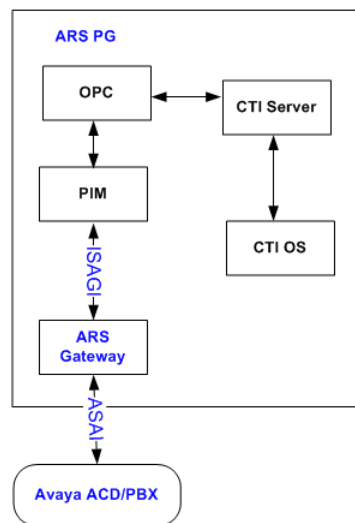
See the appropriate *System Manager Guide Supplement* for details on the interface.

- The ARS Gateway communicates to Unified ICM via the PIM by the ISAGI (ICM SoftACD Gateway Interface) protocol.

ISAGI allows the ARS PIM via the ARS Gateway to monitor and manage agent and call activity, to support queuing and call treatment, and to perform supervisor functionality.

Overview of Architecture and Core Components

Figure 1: The ARS Gateway



The Admin Workstation (AW)

An Admin Workstation (AW) is a control console with tools and resources for monitoring the activity of the system and for managing the Unified ICM software. Two of these tools are the Configuration Manager and the Script Editor.

The Unified ICM software can support multiple AWs. An AW can be located at the Central Controller site, at call center sites, or both.

FOR AN ARI DEPLOYMENT, the role of the AW remains exactly as for a traditional Unified ICME environment. It is from an AW that you will [configure \(page 38\)](#) the ARI deployment.

The CTI Server

The CTI Server is the interface between Unified ICM and client CTI applications such as agent desktops.

CTI Server reports call events and agent work state changes to the application as they occur through each stage of the call flow—from the moment a call arrives at the answering resource (the ACD/PBX) until the caller hangs up.

The CTI interface uses a CSTA message model for unsolicited call and agent state transition events. In addition to providing an unsolicited event feed, the CTI server provides the ability to perform call control functions from the desktop.

FOR AN ARI DEPLOYMENT, the CTI Server is **required** to support desktop functionality. (In a Unified ICM environment with no ARS PG, the CTI Server is optional.)

The CTI Server is [installed as a component on the ARS PG server \(page 28\)](#).

CTI OS

The CTI OS Server handles the bulk of the event and request processing and enables the deployment of the agent and supervisor desktops.

CTI OS Server is responsible for the following aspects of the CTI integration: updating call context information, determining which buttons to enable on softphones, providing easy access to supervisor features, and automatically recovering from failover scenarios.

FOR AN ARI DEPLOYMENT, the CTI OS must be [installed \(page 35\)](#) on the same server as the ARS PG.

The ACD/PBX

The ACD/PBX provides the following:

- Connections for agent phones. The ARI deployment supports only one line appearance per agent telephone. The configuration of the phone used by the ACD/PBX must match the equivalent of the one line appearance. Refer to the *System Management Supplement Guide* for details.
- Executing of virtual VRU scripts, as requested by a Unified ICM script (if required).
- Connection to the telephone network, typically by T1 or E1 lines.
- Internal Port Switching Matrix. The ACD/PBX performs the basic switching activities and notifies the Unified ICM via the PBX's proprietary interface.

The Voice Response Unit (VRU)

IN AN ARI DEPLOYMENT, call treatment and queuing are handled by a Voice Response Unit (VRU).

VRUs are computers that run Interactive Voice Response (IVR) telephony applications such as prompting for information, providing self-service features, and playing music or announcements.

Queued calls are held at a VRU until an agent is available. The VRU can also be used to handle all calls initially.

For the ARS deployment, the VRU must support the [Service Control Interface \(page 57\)](#). SCI provides the ability to prompt and collect from callers and to route parked calls out of the queue to another destination.

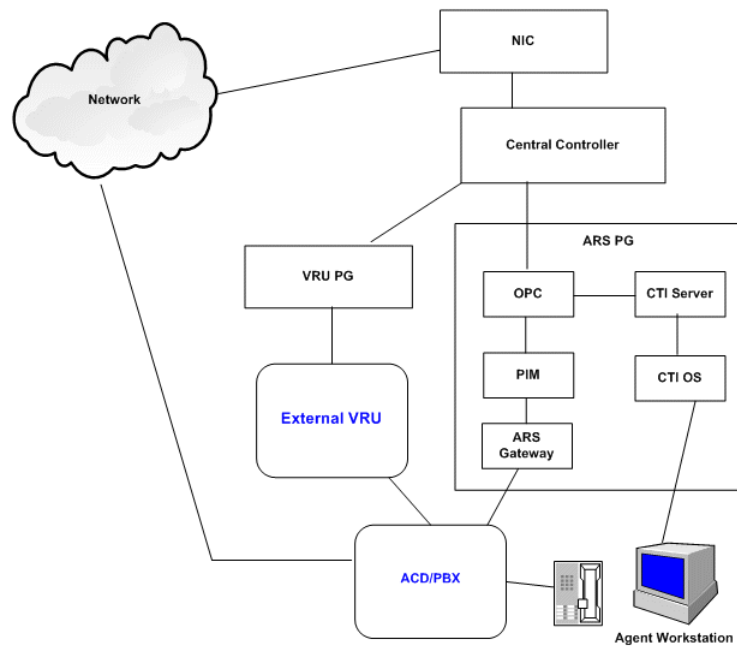
Overview of Architecture and Core Components

An ARI deployment might include either or both of these methods for call queuing and call treatment:

- An external (network) VRU within the carrier network or at the enterprise level
- A 'Virtual' VRU that is embedded within the ACD/PBX, if that functionality is supported by the ACD/PBX

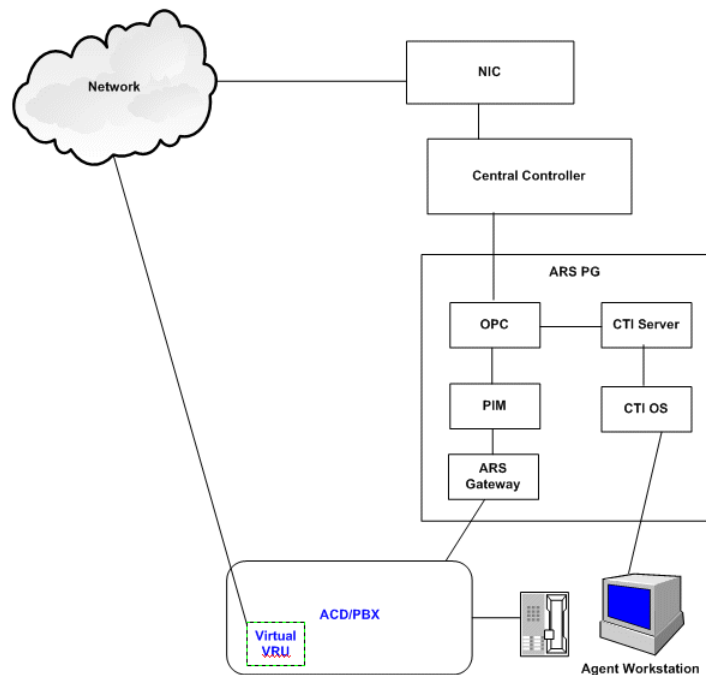
The following illustration shows an **external, network VRU**. Both the VRU PG and the ARS PG connect to the Central Controller. Translation routes move the calls between the peripherals.

Figure 2: External (Network) VRU



The following illustration shows a **Virtual VRU** embedded within the ACD/PBX.

Figure 3: Virtual (embedded) VRU



See also [Queuing \(page 57\)](#).

About the Virtual VRU

An ACD/PBX that supports Virtual VRU (VVRU) functionality can run Virtual VRU scripts as directed by ICM routing scripts. This is the case for the Avaya.

Virtual VRU functionality is controlled by the Service Control Interface (SCI) of the ISAGI protocol. Through the ARS PG and the SCI protocol, the Avaya ACD/PBX can emulate a VRU to queue calls and run VRU scripts. Since the scripts that are executed are not on a separate, physical VRU, they are referred to as Virtual VRU (VVRU) scripts.

When calls are queued to the Virtual VRU on the ACD/PBX, the ARS PG and the SCI interface “park” the calls on a Definity Vector Directory Number (VDN).

A VVRU script is a specially configured Vector Directory Number (VDN) on Avaya ACD/PBX that runs a vector to offer call treatment to the caller. The vectors might play announcements using announcement boards and play music-on-hold. When the VVRU script completes, another VDN is called that returns the result to the ICM script that executed the VVRU script.

Although VVRU scripts are not as robust as IVR scripts on a VRU, they enable basic call queuing and caller treatment. A VVRU can route internal transfers to the best resource in the enterprise. It can also distribute incoming calls in a Site ICM environment. For more extensive call treatment, you must use an external VRU.

If the Virtual VRU is used (via the SCI interface), an ASAI link is dedicated to passing routing messages between the ARS Gateway and the switch. The ASAI link is configured by the “/route”

Examples of Deployment Models for the ARI Solution

argument in the PBX Host Port Number field on the [ARS PIM configuration dialog box](#) (page 32).

The existence of one or more network (external) VRUs does not negate the use of the Virtual VRU as a queue point.

Note: Regardless of whether you use a network VRU or a Virtual VRU, you must [configure a Network VRU](#) (page 39) for the ARS peripheral to support ICM-controlled queued calls using the SCI interface.

See the *System Manager Guide Supplement* for details about Virtual VRU scripts.

Examples of Deployment Models for the ARI Solution

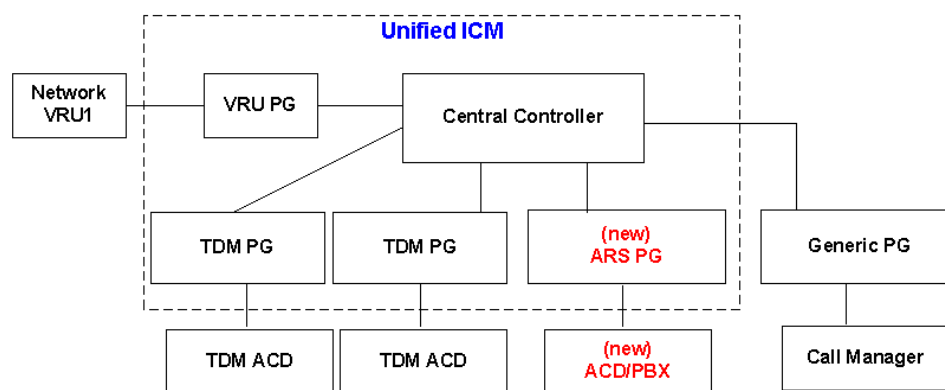
This section shows some examples of deployments and illustrates how the ARS PG fits in with the traditional Unified ICM components the same way as a traditional TDM PG.

Note that adding an ARS PG to an environment with traditional, TDM ACDs results in *hybrid* routing system. A hybrid system is one that uses both enterprise routing to TDM PGs (where the ACD picks the agent) and agent-level routing to ARS PGs (where Unified ICM picks the agent).

The *Reporting Guide for Cisco IPCC Enterprise & Hosted Editions* includes a discussion of hybrid routing.

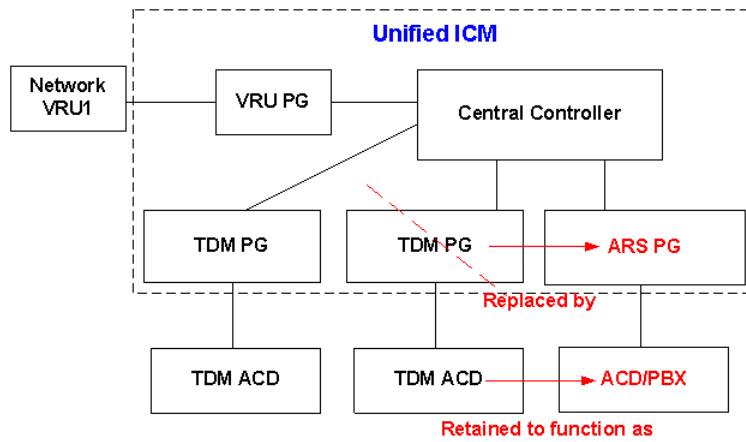
In the following illustration, an ARS PG has been added to an existing configuration that consists of TDM PGs and a Cisco Unified Communications Manager (formerly, CallManager) PG. This is a *hybrid* system.

Figure 4: ARS PG Added to Existing System



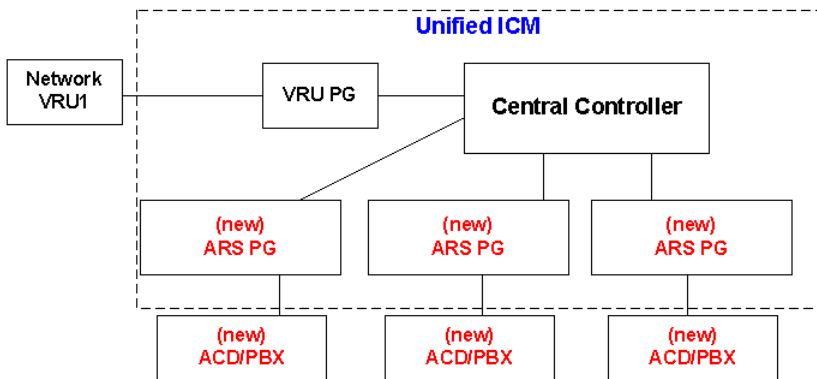
In the following illustration, an ARS PG replaces a TDM PG. The ACD is retained, and its role changes to that of an ACD/PBX. This is also a *hybrid* system, as it has both a traditional TDM PG and an ARS PG.

Figure 5: ARS PG Replaces TDM PG



This next illustration shows a Unified ICM which includes only ARS PGs. This is not a hybrid system. All routing is agent-level.

Figure 6: New Deployment with all ARS PGs



Examples of Deployment Models for the ARI Solution



Chapter 3

Installation and Configuration for the ARI Deployment

This chapter explains how to perform installation for an ARI Deployment and what parameters to set for ARI in Configuration Manager. It concentrates on those tasks that are specific to, or are different for, ARI.

For complete instructions on installation and configuration, see the *IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition* and the *ICM Installation Guide for Cisco ICM Enterprise Edition*.

Note that the values you enter during installation are 'machine' configurations and are reflected in the Registry. Values that you enter in Configuration Manager are 'database' configurations and must be in place before you can run the ARS PG.

This section contains the following topics:

- [Installation, page 27](#)
- [Configuration, page 37](#)

Installation

The pages that follow explain the installation procedure and sequence.

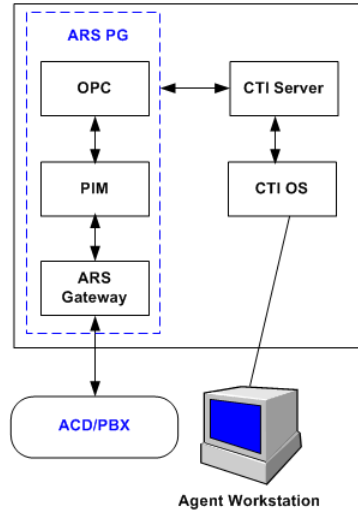
About the Server Where You Install ARS PG

The **ARS PG** must be installed on a separate, dedicated server. Both **CTI Server** and **CTI OS** must be co-located on that server. A VRU PG can also be installed on the ARS PG server.

Note: If your enterprise requires multiple ARS PGs, each must be on a unique server where CTI Server and CTI OS are also installed.

The following illustration represents an ARS PG Server on which the three components have been installed. Note that the *OPC*, *PIM*, and *ARS Gateway* are processes installed with the ARS PG.

Figure 7: Server for the ARS PG



Preparing a Server for the ARS PG

The first release in which the ARS PG is offered is Minor Release 7.2(1).

Release 7.2(1) is a Minor Release and cannot be installed directly. The dedicated server where you intend to install the ARS PG must first be installed with the base Release and then upgraded to Release 7.2(1).

(1) Bring the Server to the Base Release

For a server that is not at Release 7.0(0), use the Release 7.0(0) Media Setup to install the base release with an ICM instance.

Note: An instance is a single installation of Unified ICM software and typically consists of several components. On this ARS PG server, however, you will add *only one component*: CTI Server.

For a server that is already at Release 7.1(x), add the CTI Server component from Release 7.1 Local Setup.

If you repurpose a Release 7.1(x) server to install the ARS PG, you might need to remove components that cannot co-reside with the ARS PG. See [About the Server Where You Install the ARS PG \(page 27\)](#).

Why CTI Server is Added First

Adding the CTI Server component serves two purposes:

1. Identifies the server as a PG node. This is necessary for the Release 7.2 installer you must run subsequently.
2. Fulfills the requirement that the CTI Server be located on the same server as the ARS PG.

For installation information, see the following:

- The chapter on CTI Server Setup in the *ICM Installation Guide for Cisco ICM Enterprise Edition Release 7.0(0)*.
- *Installation Guide Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.1(1)*.

Now: You now have a Release 7.0 or 7.1(x) server with only one component—CTI Server.

Next: Your next step is to upgrade this server to 7.2(1).

(2) Upgrade to 7.2(1)

Bring your CTI Server machine to Unified ICM Release 7.2(1).

The Router, Logger, and AW must also be upgraded to Release 7.2(1) before you add the ARS PG to the server. See the *Installation Guide Cisco ICM/IPCC Enterprise & Hosted Editions Release 7.2(1)*.

Now: You now have a server at Minor Release 7.2(1).

Next: Your next step is to add the ARS PG in Configuration Manager. You do this at an Admin Workstation. This initial configuration is necessary to obtain values for the Logical Controller ID and Physical Controller ID which you will enter on the PG installation screens.

(3) Add the ARS PG in Configuration Manager

Adding and saving the ARS PG in Configuration Manager gives you the Logical Controller ID and the Peripheral ID required on the installation screens. Perform this minimal configuration to acquire these two numbers. You will complete the ARS PG configuration after the installation.

-
- | | |
|---------------|--|
| Step 1 | To access the Configuration Manager, at an Admin Workstation, select Start > Programs > ICM > Admin Workstation > Configuration Manager . |
| Step 2 | In the ICM Configuration Manager, select Configure ICM > Peripherals > Peripheral > PG Explorer . |
| Step 3 | Click Retrieve . |

Step 4 Click **Add**.

The Logical Controller tab displays at the top right side of the panel.

Step 5 Complete the Logical controller tab as follows:

- a. **Logical controller ID** and **Physical controller ID**: These fields appear as UNASSIGNED. Values are assigned by the system when you click **Save**.
- b. **Name**: Enter a unique name for the PG that identifies it as an ARI deployment.
- c. **Client Type**: Select *Agent Routing Service*.

Step 6 Click **Save**.

Once the record is saved, the Logical controller ID appears on the Logical controller tab and the Peripheral ID appears on the Peripheral tab.

Figure 8: Logical Controller ID

Logical Controller

Logical controller ID: * 5000 Physical controller ID: * 5000

Name: * ARIPG

Client type: * Agent Routing Service

Figure 9: Peripheral ID

Peripheral Advanced Agent Distribution

Peripheral ID: * 5000

Make a note of them. You will need to enter them during the installation.

Step 7 Close the screen and exit Configuration Manager.

Now: You have now done basic configuration for the ARS PG, which provides you with ID numbers you supply during installation. [You will complete the PG configuration after the installation \(page 42\).](#)

Warning: Do not attempt to bring the PG up. The configuration is not complete, and you will see errors until you complete the configuration.

Next: Your next step is to install the ARS PG. You do this by running the local ICM setup.

Installing the ARS PG on the Server

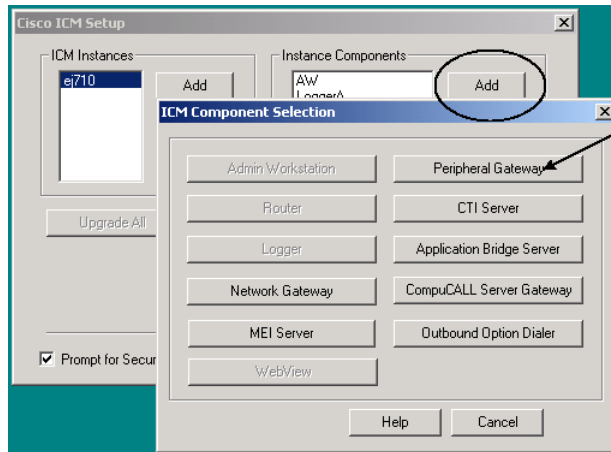
Once the server machine is at Release 7.2(1), install the ARS PG following these steps.

- Step 1** At the CTI Server machine which is installed to Release 7.2, run `icmsetup.exe` from the `icm\bin` folder (**Start Run icmsetup**).
- Step 2** From the initial Cisco ICM Setup dialog box, select the ICM Instance in the left column. Then click the **Add** button to the right of the Instance Components column.

This opens the ICM Component Selection dialog box.

- Step 3** At the ICM Component Selection dialog box, select **Peripheral Gateway**.

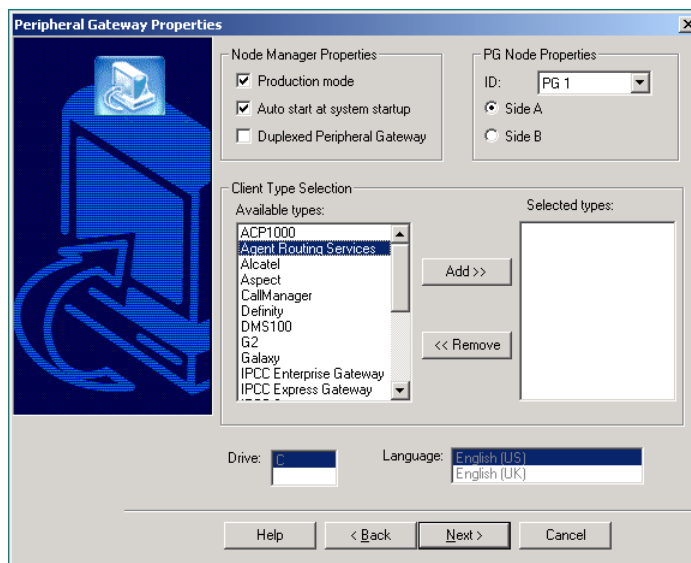
Figure 10: Setup: Select PG Component



This opens the Peripheral Gateway Properties screen.

- Step 4** At the Peripheral Gateway Properties screen, locate Agent Routing Services in the Client Type Selection column. Click **Add >>** to move it to the Selected Types column.

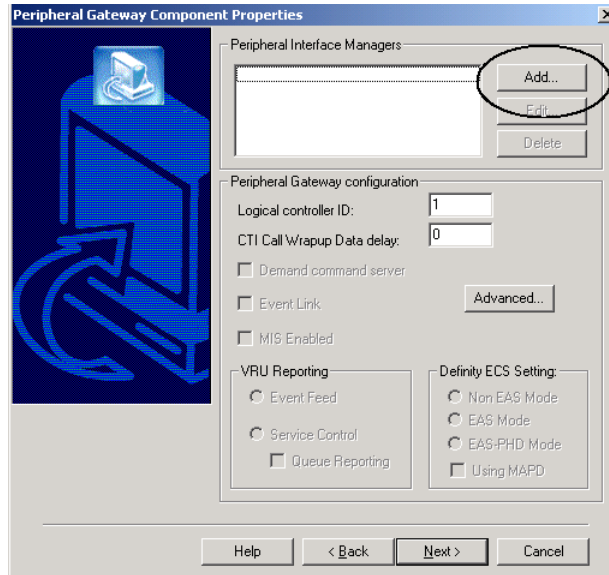
Figure 11: Setup: Select ARS Client Type



Note: No Client Type other than the Agent Routing Services Client Type can be added to the PG.

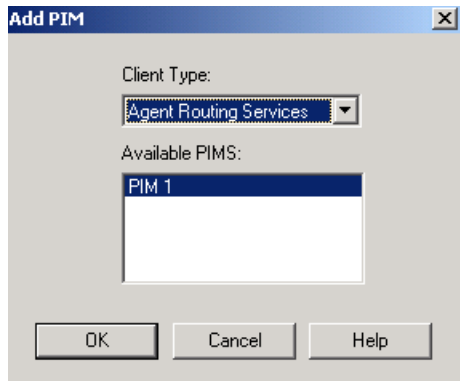
Step 5 Click **Next** to open the Peripheral Gateway Component Properties screen.

Figure 12: Peripheral Gateway Component Properties



Step 6 Click **Add** to open the Add PIM popup and then click **OK**.

Figure 13: Setup: Add PIM popup



This opens the ARS PIM Configuration dialog box.

Step 7 Complete the ARS PIM Configuration dialog box as follows:

Figure 14: Setup: ARS PIM Configuration dialog box



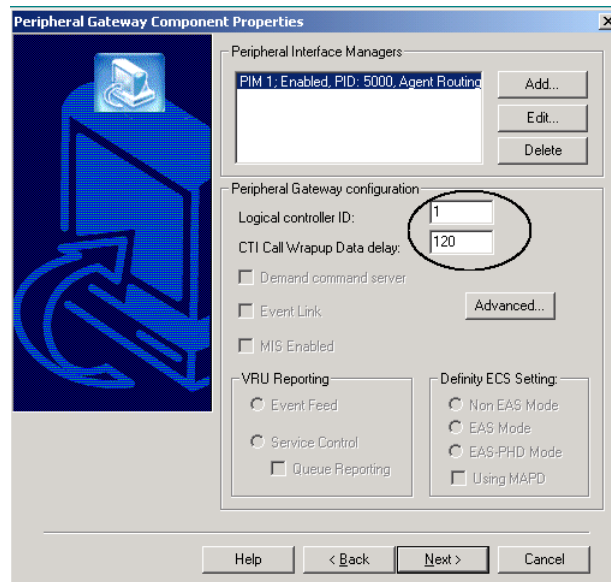
- a. Check the **Enable** checkbox. The ARS PIM will not run if this box is unchecked.
- b. The **Peripheral Name** defaults.
- c. **Peripheral ID:** enter the ID for the peripheral. [This ID value was created when you added the ARS PG in Configuration Manager. \(page 30\)](#)
- d. **Gateway Provider** defaults to Cisco.
- e. **Cisco Gateway Type** defaults to Avaya.
- f. **PBX Host Name:** Enter the Host name or IP address of the Server where the gateway will connect via ASAI links. Valid numbers are from 1 to 8.
- g. **PBX Host Port Number:** Enter the ASAI link number(s) used for event and routing communications. Examples of valid values for this field are `/event 1` and `/event 1,2 /route 3`
 - The `/event` tag is used to indicate one or more ASAI links used for event notification and call control. Use commas to delimit multiple link numbers (`/event 1,3,5`). Use a dash to indicate a range (`/event 1-4`)
 - The `/route` tag is used to indicate the ASAI link used for SCI support via routing. Valid values include a single number from 1 to 8.
- h. The **Gateway Host Name** defaults to the Local Host Name and is greyed out.
- i. The **Gateway Host Port Number** defaults to 6101. You can change it if this port is used by another application.

Step 8 Click **OK**.

This closes the ARS PIM Configuration screen and returns you to the Peripheral Gateway Component Properties screen.

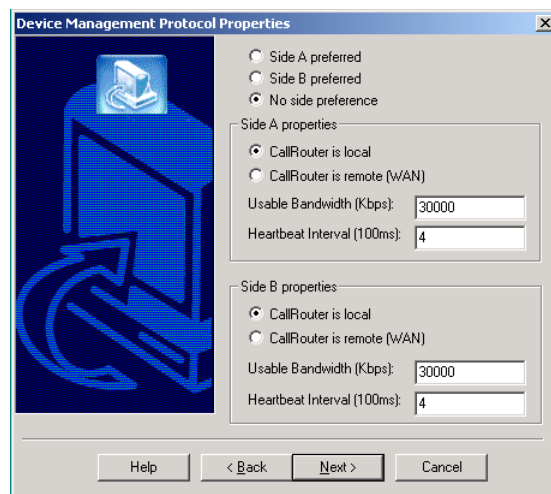
- Step 9** Make two final configurations on the Peripheral Gateway Component Properties screen:
- Enter the **Logical controller ID** from the Logical_Interface_Controller record for the PG. [This ID value was created when you added the ARS PG in Configuration Manager. \(page 30\)](#)
 - For **CTI Call Wrapup Data Delay**, enter the number of seconds the PG waits for the CTI client to send data after the agent finishes call wrap up.

Figure 15: Setup: Peripheral Gateway Component Properties



- Step 10** Click **Next** to open the Device Management Protocol Properties screen.

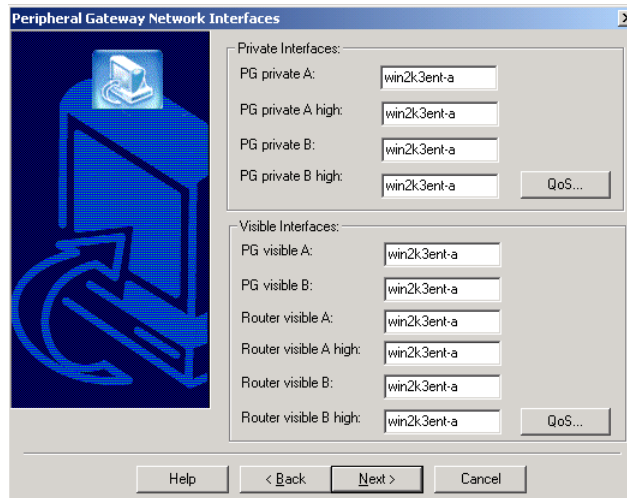
Figure 16: Setup: Device Management Protocol Properties



Accept the defaults, or change the configuration if necessary. Refer to the **Help** for field descriptions.

Step 11 Click **Next** to open the Peripheral Gateway Network Interfaces screen.

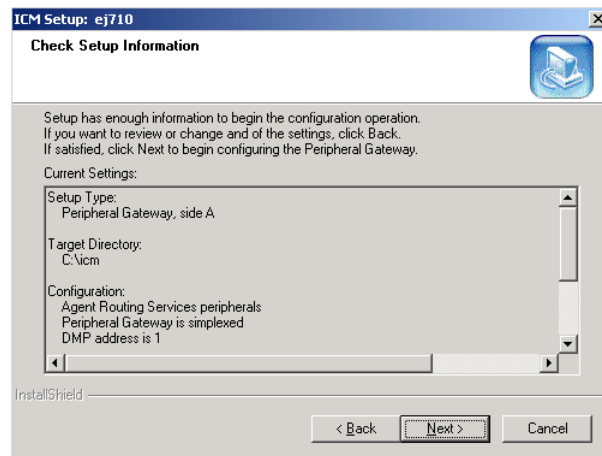
Figure 17: Setup: Peripheral Gateway Network Interfaces



Accept the defaults, or change the configuration if necessary. Refer to the **Help** for field descriptions.

Step 12 Click **Next** to open the Check Setup Information screen.

Figure 18: Setup: Check Setup Information



Step 13 Review your selections. Click **Back** to make revisions, or click **Next** to complete the PG configuration

Installing CTI OS Server on the ARS PG Server Machine

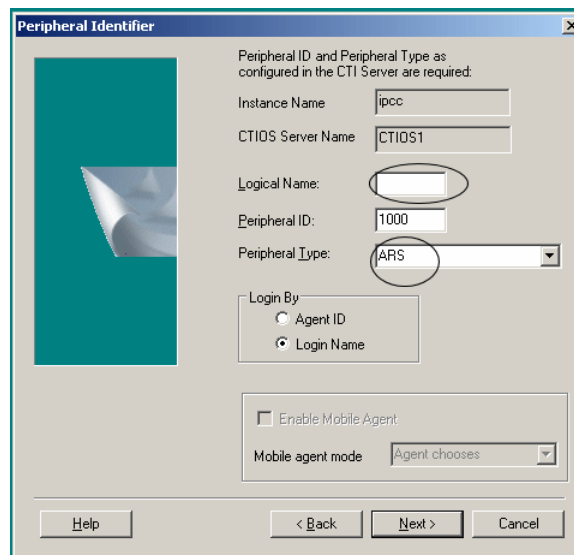
Install CTI OS Server co-resident with the ARS PG.

Step 1 Install CTI OS Server 7.0 on the PG machine.

Installation

- Step 2** At the Peripheral Identifier screen, where you are required to select a Peripheral Type, ARS will not be listed. Select another Peripheral Type, such as IPCC System.
- Step 3** Complete the installation.
- Step 4** Apply the CTI OS 7.2(1) Patch.
- Step 5** Run local setup from the icm\ctios_bin directory.
- Step 6** Edit the server to change the Peripheral Type from the choice you made in Step 2 to **ARS**.
- Step 7** Edit the Logical Name field to match the changed peripheral type.

Figure 19: CTI OS Peripheral Identifier Screen



For complete information on installing CTI OS, see the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.2(1)*.

Installing the Agent and IPCC Supervisor Desktops

Perform this procedure at each agent and supervisor computer.

- Step 1** From the Install\CTIOSClient directory on the CTI OS CD, run **Setup.exe**.
- Step 2** Click **Next** on the Welcome screen to open the Software License Agreement screen.
- Step 3** Click **Yes** to accept the agreement.
- This opens the Choose Destination Location screen.
- Step 4** Accept the default drive or click **Browse** to specify another drive.
- Step 5** Click **Next** to open the Select Components screen.

- Step 6** Select (check) the CTI Toolkit Desktop Client component that you want to install: *Agent Desktop* or *IPCC Supervisor Desktop*.
- Step 7** Click **Next** to open the CTI OS Server Information screen.
- Step 8** Enter the Name or IP Address and the Port Number for your CTI OS systems.
- Step 9** Click **Next** open the Start Copying Files screen.
- Step 10** Click **Next** to begin the installation.
- When installation is complete, you are prompted to install the Security feature.
- Step 11** Click **OK** to configure CTI OS security.
- Step 12** At the Setup Complete screen, specify whether or not you want to restart your computer. Then click **Finish** to exit Setup.

For complete information on installing CTI OS, see the *CTI OS System Manager's Guide for Cisco ICM/IPCC Enterprise & Hosted Editions, Release 7.2(1)*.

Configuration

Special configuration is required in both ICM Configuration Manager and on the ACD/PBX to support ARI functionality.

This guide explains configuration that you define in Unified ICM [Configuration Manager \(page 38\)](#).

In order for Unified ICM to route calls to the ACD/PBX, you must complete the following configuration:

- [Configure a Network VRU for the ARS PG. \(page 39\)](#)
- [Configure Agent Desk Settings for agents associated with the ARS PG. \(page 40\)](#)
- [Configure the ARS PG \(page 42\)](#)
- [Configure the ARS PG Peripheral. \(page 43\)](#)
- [Configure Agent Targeting Rules. \(page 49\)](#) if you will use them.
- [Configuring for Reporting \(page 51\)](#)
- **Other Configurations**
 - [Agents \(page 52\)](#)
 - [Skill Groups \(page 53\)](#)

Configuration

- [Services \(page 54\)](#)
- [Network Trunk Groups and Trunk Groups \(page 54\)](#)
- [Dialed Numbers \(page 55\)](#)
- [Device Targets \(page 55\)](#)
- [Translation Routes \(page 55\)](#)

About ACD/PBX Configuration

The configuration on the ACD/PBX varies per ACD/PBX. For the Avaya, it includes configuration of:

- One or more ASAI links
- Agent devices (stations)
- One and only one agent skill group that all agents log in to
- Feature access codes for the hard phones, if used
- VDN and vectors used for the Service Control Interface: call treatment, post-routing, queuing, and other processing of calls

It is important to keep your ICM configuration aligned with your ACD/PBX configuration. Changes and additions, such as those to agents and agent telephones, need to match.

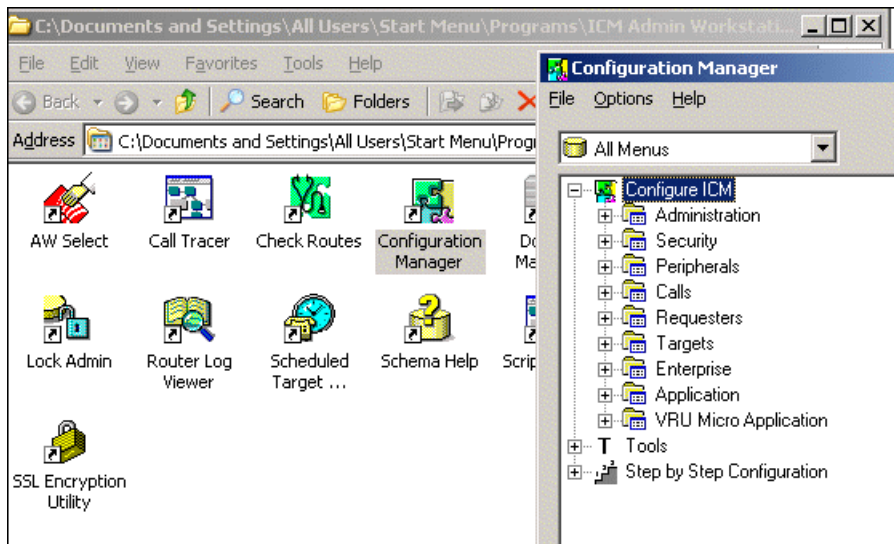
See the appropriate *System Manager Guide Supplement* for details on ACD/PBX configuration.

About Configuration Manager

Configuration that you perform for Unified ICM is done from Configuration Manager. Configuration Manager is a utility on all Admin Workstations that you use to add, save, and edit configuration settings.

To access the Configuration Manager, at an Admin Workstation, select **Start > Programs > ICM > Admin Workstation > Configuration Manager**.

Figure 20: Configuration Manager



Configuring a Network VRU

You *must* configure a Network VRU before you can configure and save the ARS Peripheral.

For an ARI deployment, configure a *Type 9 VRU* whether you will use an external VRU or Virtual VRU scripts. If you do not configure a Type 9 network VRU, post-routed and translation-routed calls will fail.

When you configure the ARS PG Peripheral, you will specify the Type 9 Network VRU at the [Advanced tab \(page 45\)](#).

-
- Step 1** In the Configuration Manager, select **Configure ICM > Targets > Network VRU > Network VRU Explorer**. The Network VRU Explorer dialog box opens.
- Step 2** Click **Retrieve**.
- Step 3** Click **Add**.
- Step 4** Complete the Network VRU tab:
- For **Name**, enter a suitable name.
 - For **Type**, choose Type 9.
- Note:** The Network VRU must be “Type 9”. No other Network VRU Type is accepted.
- Refer to the online help for other field explanations.
- Step 5** Click **Save** and then click **Close**.
-

Figure 21: Configuring Network VRU

The screenshot shows a configuration window for 'Network VRU'. It has two tabs: 'Network VRU' and 'Network VRU Banks'. The 'Network VRU Banks' tab is selected. There are three fields: 'Name' with a text input containing 'ARI_PG', 'Type' with a dropdown menu showing 'Type 9', and 'Description' with an empty text input. The 'Name' and 'Type' fields have an asterisk next to them, indicating they are required.

Note: If you intend to use an external VRU (a VRU connected to Unified ICM through an VRU PG and not connected to the ARS PG through the ACD/PBX), repeat these steps to configure a second VRU for that purpose. The external VRU will be a *Type 2* VRU.

Configuring Agent Desk Settings

You may or may not already have Agent Desk Settings that are appropriate for the agents who will be configured for the ARS PG. If you do not, or if you are unsure, you *must* configure Agent Desk Settings before you can configure and save the ARS Peripheral.

When you configure the ARS PG Peripheral, you need to specify default desk settings at the [Peripheral tab \(page 44\)](#).

Agent Desk Settings associate a set of permissions or characteristics with specific agents. The settings are comparable to Class of Service settings on a PBX or ACD.

When you configure Agent Desk Settings, you specify the amount of non-active time after which an agent is automatically logged out, whether wrap up is required following incoming and outbound calls, the amount of time allocated for wrap up, and the method used for assist and emergency calls.

Desk settings are associated with an agent when the agent is configured. They are global in scope and can be applied to any configured agent on any peripheral within a Unified ICM configuration.

Note: The Agent Desk Setting that is selected for the peripheral is assigned to all agents under this peripheral. If an agent is explicitly assigned another Agent Desk Setting in Agent Explorer, then *that* setting overrides the Agent Desk Setting selected for the ARS Peripheral.

-
- Step 1** From the Configuration Manager, choose **Configure ICM > Enterprise > Agent Desk Settings > Agent Desk Settings List**. The ICM Agent Desk Settings List dialog box opens.
- Step 2** Click **Retrieve** and then **Add**.
- Step 3** Complete the Attributes tab:
- For **Name**, enter a name that can be recognized as an ARI Desktop.
 - Ring no answer** fields: Leave blank. (RONA is not supported for the ARS PG.)

- c. **Logout non-activity Time:** Enter the number of seconds (between 10 and 7200) in which the agent can be in a not ready state before the Unified ICM automatically logs out the agent.
- d. **Work Mode on Incoming.** Indicates whether wrap up is required or possible following an incoming call. Select Required, Optional, Not Allowed, or Required from the drop-down list.
- e. **Work Mode on Outgoing:** Select one of the three options: Optional, Not Allowed, or Required.
- f. **Wrap Up Time.** Enter the number of seconds allowed for the agent to wrap up the call.
- g. **Assist Call Method.** Select consultive call or blind conference from the drop-down list to indicate whether the ARS PG will create a consultive call or a blind conference call for the supervisor assistance request.
- h. **Emergency Alert Method.** Select consultive call or blind conference from the drop-down list to indicate whether the ARS PG will create a consultive call or a blind conference call for the emergency call request.
- i. **Description.** Enter additional optional information about the agent desk settings.
- j. **Miscellaneous**

Use the following boxes to select or de-select miscellaneous settings for an agent. Click on the box to enable/disable the setting.

- **Auto-answer.** Indicates whether calls to the agent will be answered automatically. The agent is not required to take any action to answer the call.
 - **Idle reason required.** Indicates whether an agent is required to enter a reason before entering the Idle state.
 - **Logout Reason Required.** Indicate whether the agent is required to enter a reason before logging out.
 - **AutoRecord on Emergency.** Not supported for ARI.
- k. **Outbound Access:** Not supported for ARI.

Step 4 Click **Save** and then click **Close**.

Note that the Cisco Unified Mobile Agent field is not applicable for an ARI deployment. Leave Enable Cisco Unified Mobile Agent unchecked.

Figure 22: Configuring Agent Desk Settings

The screenshot shows the 'Attributes' configuration window for an Agent Desk. The settings are as follows:

- Name: *ARIDesktop
- Ring no answer time: [] seconds (1 - 120)
- Ring no answer dialed number: <None>
- Logout non-activity time: [] seconds (10 - 7200)
- Work mode on incoming: *Optional
- Work mode on outgoing: *Optional
- Wrap up time: 7200 seconds (1 - 7200)
- Assist call method: Consult
- Emergency alert method: Consult
- Description: []
- Miscellaneous:
 - Auto answer
 - Idle reason required
 - Logout reason required
 - Auto record on emergency
- Outbound Access:
 - International
 - National
 - Local private network
 - Operator assisted
 - PBX
- Enable Cisco Unified Mobile Agent
 - Mobile agent mode: Agent chooses

Configuring the ARS PG

You added and saved the ARS PG before the installation to obtain the IDs required on the installation screens. In this step, you complete the configuration screens for the ARS PG and the ARS Peripheral.

-
- Step 1** In the ICM Configuration Manager, select **Configure ICM > Peripherals > Peripheral > PG Explorer**.
- Step 2** Click **Retrieve**.
- Step 3** [Select the ARS PG you created before the installation. \(page 29\)](#)
- The Logical Controller tab displays at the top right side of the panel.
- Step 4** Complete the Logical controller tab as follows:
- Logical controller ID** and **Physical controller ID**: These fields were assigned by the system when added the PG.
 - Name**: Enter a unique name for the PG that identifies it as an ARI deployment.
 - Client Type**: Select *Agent Routing Service*.
 - Configuration parameters**: Leave blank.
 - Description** and **Physical controller description**: Enter information to describe the PG and the physical controller.

- f. **Primary CTI address** in either dotted numeric or name format. As the CTI server is installed at the PG, enter the PG address.
- g. **Secondary CTI address:** The secondary CTI address is needed if a CTI server is installed at the PG and the ICM system is duplexed.

Figure 23: Configuring the PG

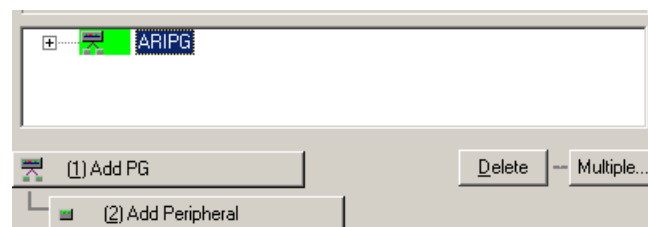
Configuring the ARS PG Peripheral: Peripheral Tab

Agents are grouped by assigning them to a peripheral, independent of their physical location. Unified ICM uses the peripheral assignment for call handling and administrative purposes.

You need to configure the ARS PG Peripheral so that you can associate agents, skill groups, and services with it.

- Step 1** In the ICM Configuration Manager, select **Configure ICM > Peripherals > Peripheral > PG Explorer**.
- Step 2** Click **Retrieve**.
- Step 3** Highlight the ARS PG icon in the tree hierarchy in the left panel.
- Step 4** Click **Add Peripheral** (lower left side of the dialog box).

Figure 24: Configuring the PG Peripheral



This displays a panel with seven tabs at the lower right of the dialog box, beneath the Logical Controller tab.

At the **Peripheral** tab, enter values as follows:

Figure 25: Configuring the PG Peripheral: Peripheral Tab

Skill Group Mask	Routing client	Default route	Peripheral Monitor
Peripheral	Advanced	Agent Distribution	
Peripheral ID:	* 5000		
Name:	* ARIPG_1		
Peripheral name:	* ARIPG_1		
Client type	* Agent Routing Service		
Location:			
Abandoned call wait time:	* 5		
Configuration parameters:			
Call control variable map:			
Default desk settings:	ARIDesktop		
Peripheral service level type:	* Calculated by Call Center		
Description:			
Enable post routing:	<input checked="" type="checkbox"/> Peripheral auto configured: <input type="checkbox"/>		

- Step 5** **Name.** An enterprise name for this peripheral. The name must be unique among all peripherals in the enterprise.
- Step 6** **Peripheral name.** The name of the peripheral as it is known at the site. Unlike the Enterprise Name field, the value of this field does not have to be unique.
- Step 7** **Client type.** The type of the peripheral. The value for this field (Agent Routing Services) defaults from the default from values you entered when you configured the PG. Do not change to another client type - client type must be Agent Routing Services.
- Step 8** **Location.** The peripheral's location. For example: the name of a city, building, or department.
- Step 9** **Abandoned call wait time.** Minimum time in seconds an incoming call must be queued before being considered an abandoned call if the caller hangs up.
- Step 10** **Configuration parameters.** A string containing any parameters that must be sent to the device to initialize it. Refer to the instructions in the specific PBX supplement for instructions on completing this field.
- Step 11** **Call Control Variable Map.** Leave blank.
- Step 12** **Description.** Additional information about the peripheral.
- Step 13** **Default desk settings.** select [the Agent Desk Setting you have configured \(page 40\)](#).
- Step 14** **Peripheral service level type.** This is greyed out and cannot be selected.
- Step 15** **Service level type.** This field is not available.
- Step 16** **Service level threshold.** This field is not available.
- Step 17** **Enable post routing.** This must be enabled (checked).

Complete the remaining tabs as explained in the following sections.

Caution: You can configure only one peripheral for each ARS PG. To configure a second peripheral, you need to install a second ARS PG.

Configuring the ARS PG Peripheral: Advanced Tab

At the **Advanced** tab:

Figure 26: Configuring the PG Peripheral: Advanced Tab

Skill Group Mask	Routing client	Default route	Peripheral Monitor
Peripheral	Advanced	Agent Distribution	
Available holdoff delay: *	0		
Answered short calls threshold:	0		
Network VRU:	ARI_PG		
Agent auto-configuration:	<input type="checkbox"/>	Internal IPTA Only:	<input type="checkbox"/>
Agent targeting mode: *	Rule Preferred		

Step 1 **Available holdoff delay:** Set this field to 0.

Step 2 **Answered short calls threshold:** Maximum duration, in seconds, for a short call. Any calls with a duration under the threshold are considered short. This field will track agents who hang up on callers.

Step 3 For **Network VRU**, select [the Type 9 Network VRU you have configured \(page 39\)](#).

Note: It is important to select the Type 9 Network VRU. You can save the ARS PG without selecting a Network VRU, but call routing fails without this Network VRU configuration, if the request is originated from the ARS Peripheral.

Step 4 Do not check **Internal IPTA Only**.

Step 5 For **Agent targeting mode**, options are as follows:

a. **Device Target Preferred**

The existing device target selection is used to determine the label. This is the default for systems upgraded from an earlier release. Device targets are used to find labels, just as in earlier releases. Rules can be configured, as part of a strategy to switch over to them, but they are ignored.

If you make this selection, you must [configure Device Targets \(page 55\)](#).

b. **Rule Preferred**

This is the default option for newly-created peripherals. If you retain this selection, you must have [configured Agent Targeting Rules \(page 49\)](#).

Configuration

The rules are used to create the label. The CallRouter uses the Agent Targeting Rule if one exists. If no rule exists, the CallRouter then determines if a device target has been configured. If there is no Agent Targeting Rule and a device target has been configured, the CallRouter uses the device target for routing the call. If no device target has been configured and no rule exists, the routing of the call fails.

c. Rules compare to existing Device Target

This option is available to assist customer testing of newly created rules for a peripheral that previously used device targets.

Step 6 Refer to the online help to complete the other fields on this tab.

Configuring the ARS PG Peripheral: Agent Distribution and Skill Group Mask Tabs

At the **Agent Distribution** tab:

Figure 27: Configuring the PG Peripheral: Agent Distribution Tab

Skill Group Mask	Routing client	Default route	Peripheral Monitor
Peripheral	Advanced	Agent Distribution	
Enable agent reporting <input checked="" type="checkbox"/>		Agent event detail <input checked="" type="checkbox"/>	
Agent Distribution Entries			
Distributor Site Name			Enabled <input type="checkbox"/>

Step 1 Check **Enable agent reporting**.

Step 2 Check **Agent event detail**

Step 3 **Distributor Site Name:** Click **New** and enter the site name of the Admin Workstation to which the Unified ICM router and logger should send agent information. Note that the site name of the AW distributor is the same name that is entered during AW distributor set up. If nothing is entered for the site name during installation, this defaults to the host name.

Step 4 At the **Skill Group Mask** tab, no configuration is required for the ARI Deployment. Sub-skill groups are not supported for ARI.

Configuring the ARS PG Peripheral: Routing Client Tab

At the **Routing Client** tab:

Figure 28: Configuring the PG Peripheral: Routing Client Tab

Peripheral	Advanced	Agent Distribution
Skill Group Mask	Routing client	Default route Peripheral Monitor
Name:	* ARIPG	ID: * 5000
Timeout threshold:	* 1500	
Late threshold:	* 500	
Timeout limit:	* 10	
Default media routing domain:	NONE	
Default call type:	NONE	
Configuration parameters:		
Use DN/Label map:	<input type="checkbox"/>	
Client type:	* Agent Routing Service	
Description:		
Network routing client:		
Network transfer preferred:	<input checked="" type="checkbox"/>	

-
- Step 1** **Name:** An enterprise name for this routing client. The name must be unique among all routing clients in the enterprise.
- Step 2** **Timeout Threshold:** The maximum time, in milliseconds, the routing client can wait for a response to a routing request. The NIC sends a default response slightly before this threshold.
- Step 3** **Late Threshold:** The threshold value, in milliseconds, for classifying responses as late. Any response that exceeds this threshold is considered late even if it does not exceed the TimeoutThreshold.
- Step 4** **Timeout Limit:** The maximum time, in seconds, for which the routing client waits for a response. If the routing client receives no responses within this limit, it terminates routing operation.
- Step 5** For **Default media routing domain**, select None or Cisco_Voice.
- Step 6** For **Default call type**, select the call type used for routing a call from this routing client in the event the call cannot be categorized into any other Call Type defined in the system.
- Step 7** Be sure **Client Type** is Agent Routing Service.
- Step 8** Optionally, select (check) **Network transfer preferred**.
-

Configuring the ARS PG Peripheral: Default Route Tab

At the **Default Route** tab:

Figure 29: Configuring the PG Peripheral: Default Route Tab

- Step 1** The **Media routing domain**, defaults to Cisco_Voice.
- Step 2** For **Route**, no default route selected. Route selection is not mandatory.

Configuring the ARS PG Peripheral: Peripheral Monitor Tab

A peripheral monitor entity is defined as a physical resource that exists in the ACD/PBX to be monitored by Unified ICM.

Peripheral Monitors are used to designate three classes of objects for the ARS Gateway. Depending on your requirements, you might need to configure some or all of these classes of objects, which are:

1. **The skill group/hunt group defined on the Avaya ACD/PBX that agents can log in to for hard phone support.**

This extension is configured as a method to inform the ARS PG at startup that the ACD/PBX skill group should be monitored to detect when agents log in or log off via their hard phones.

Each agent configured on the ACD/PBX must be assigned to one and only one ACD/PBX skill group/hunt group.

This skill is monitored by Unified ICM by the peripheral monitor configuration: type= station, extension = split extension, parameter = VDN_SKILL.

Enter only one VDN_SKILL in the Peripheral Monitor tab.

2. **The Avaya VDNs that are used for routing.** This includes the Virtual VRU script VDN. The extensions of these objects require an appropriately configured VDN on the ACD/PBX.

A VDN is an extension on the switch that does not terminate at an actual device. It is an internal end-point that can take a call and perform programmable actions with the call.

3. **The hard phone extensions, required when Agent Targeting Rules are used for routing.**

Extensions are monitored at startup and are reported to the PIM by the ARS Gateway to detect when agents log in or log off via their hard phones. Having the extension in the Peripheral Monitor tab enables the synchronization of the hard phones and the softphones.

For Agent Targeting Rules functionality, entering the range of extensions on this tab takes the place of configuring individual Device Targets for hard-phone monitoring.

Note: DO NOT configure extensions in both the Peripheral Monitor tab and as DeviceTargets. Extensions configured in the Peripheral Monitor tab can be used only for agent targeting rule routing. They will not work for regular Unified ICM routing to agents.

To configure the extensions:

- Specify a contiguous range by providing a high and low values separated by a space.

Non-contiguous ranges must be specified by entering distinct peripheral monitor tab values.

- The configuration string is `/RANGE <lowExtension> <highExtension> / MONITOR y/HARDPHONE 2`

Hardphone Level 2 is required to ensure synchronization between the agent's softphone and the agent's teleset device.

To configure only one extension, enter the same parameter for the `<lowExtension>` and `<highExtension>`.

Figure 30: Configuring the PG Peripheral: Peripheral Monitor Tab

Peripheral		Advanced		Agent Distribution	
Skill Group Mask	Routing client	Default route	Peripheral Monitor		
Current peripheral monitor entries:					
Type	Extension	Config. Param.			
VDN	3053	VDN_USSCRIPT			
VDN	3054	VDN_ISCRIPT			
VDN	3055	VDN_READY			
VDN	3056	VDN_SCRIPT_RESULT			
VDN	3057	VDN_BUSY			
VDN	3058	VDN_RING			
VDN	3059	VDN_DISCONNECT			
Station	4071	VDN_SKILL			

Configuring Agent Targeting Rules

Once the ARS Peripheral is saved, you can configure Agent Targeting Rules. You need to do this if you specified you specify agent targeting mode at the [Advanced tab \(page 45\)](#) during the ARS PG configuration.

Note: You can configure Agent Targeting Rules only after the ARS PG is saved.

When you configure the ARS PG, you specify agent targeting mode at the [Advanced tab \(page 45\)](#).

Options are *Device Targets Preferred*, *Rules Preferred*, and *Rules compare to existing Device Target*.

If you selected *Rules Preferred* (which is the default for newly-created peripherals), then you might need to configure Agent Targeting Rules if you have not already done so.

Agent Targeting Rules allow you to configure ICM call routing by specifying the agent extension range, instead of configuring device targets and labels for every phone and for every routing client.

Although it is also possible to target agents using device targets, you might prefer to use agent targeting rules, as this method simplifies the call routing configuration.

-
- Step 1** In the Configuration Manager, select **Configure ICM > Targets > Device Target > Agent Targeting Rule**.
- Step 2** Click **Retrieve**. Then click **Add** to display the Attributes tab.
- This tab has three sections.
- Step 3** For **Name**, enter a name for the rule.
- Step 4** For **Peripheral**, select the peripheral with which the rule is associated.
- Step 5** For **Rule type**, select one of the three options:
- **Agent Extension Rule** - for routing calls to a peripheral from a routing client which does not need any prefix.
- Substitute Agent Extension Rule** - for routing calls from a routing client that requires a prefix. Requires creating DID numbers for each agent logged in.
- Translation Route Rule** - for routing calls from a routing client to a peripheral that involves a Translation Route. The Router creates a label consisting of a DID number that is shared to all calls and that ICM translates to an agent extension using the translation route feature. This fixed set of DIDs, shared among agents, reduces cost. Requires the [configuration of a translation route \(page 55\)](#) between the origin and the destination.
- Step 6** For **Translation route**: If you select Translation Route as the Rule Type, you must select one of the pre-configured translation routes from Translation route field. The translation route must be already [configured \(page 55\)](#).
- Step 7** For **Agent extension prefix and Agent Extension Length**:, If you select Substitute Agent Extension as the Rule Type, you enter values for the agent extension prefix and agent extension length.
- Step 8** For **Description**, enter a description for this rule.
- Step 9** The **Routing client** field displays the routing clients associated with the rule being added. You can add or remove routing clients for this rule.

Step 10 The **Extension Ranges** field shows the ranges of extension the Agent Targeting Rule applies to. The extension ranges are used to create labels as specified by the selected Rule Type. You can add, edit, and remove extension ranges.

Step 11 Click **Save** and then click **Close**.

Figure 31: Configuring Agent Targeting Rules

The screenshot shows the 'Attributes' configuration window for an Agent Targeting Rule. The fields are as follows:

- Name: * ARI_ATR
- Peripheral: * ARIPG_1
- Rule type: * Translation Route
- Translation route: SIPCC_2_ARI_TR
- Agent extension prefix: (empty)
- Agent extension length: 1
- Description: (empty)

Below the main fields are two sections:

- Routing client:** A table with columns 'Name' and 'Description'. It contains one entry: SIPCC_RC.
- Extension Ranges:** A table with columns 'Low Extension' and 'High Extension'. It contains one entry: 6601 and 6610.

Configuring for Reporting in an ARI Deployment

When you deploy an ARS PG, you will use the WebView IPCC reporting templates for that PG.

If you are familiar with configuring reporting for a Unified ICM environment, know that, for the most part, configuration for ICM reports and IPCC reports is identical.

The *Reporting Guide for Cisco IPCC Enterprise & Hosted Editions* has detailed information on Unified Contact Center (IPCC) reporting.

There is one configuration that affects certain IPCC Call Type reports and which is not used in ICM. This configuration is for *bucket intervals*. Bucket intervals are associated with Call Types and allow you to track data for calls abandoned or answered within specific time increments.

You can find the procedure to configure bucket intervals in the *IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition*

Notes on Other Configuration

Other configuration you might need to perform or modify when you set up the ARS PG includes:

- [Agents \(page 52\)](#)
- [Skill Groups \(page 53\)](#)
- [Network Trunk Groups and Trunk Groups \(page 54\)](#)
- [Dialed Numbers \(page 55\)](#)
- [Device Targets \(page 55\)](#)
- [Translation Routes \(page 55\)](#)

These configurations are explained in the *IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition* and the *Reporting Guide for Cisco IPCC Enterprise & Hosted Editions*.

The information that follows notes any configuration parameters to be aware of for ARI.

As you perform standard configuration, be sure to **select the ARS Peripheral or Routing Client** when you retrieve and add items to configure:

Figure 32: Select the ARS PG when Configuring

The screenshot shows a dialog box titled "Select filter data". It has a "Peripheral" dropdown menu with "ARIPG_1" selected, which is circled in red. Below this are three dropdown menus: "Optional Filter" (set to "None"), "Condition", and "Value". At the bottom, there are three buttons: "Save" (with a checkbox), "Retrieve", and "Cancel filter changes".

Agents

In a traditional Unified ICM configuration, agents associated with an ACD are dynamically configured by the TDM PG.

For an ARI Deployment, agents must be statically configured in the ICM database. The static configuration defines the characteristics of an agent, as well as the address of the agent for call delivery.

You also need to set up agents on the ACD/PBX for hard phone support and all agents configured in the ACD/PBX configuration must be added to one and only one skill group.

To configure an agent, from Configuration Manager, click **Configure ICM > Peripherals > Agent > Agent Explorer**. Click **Retrieve** and then **Add**.

Complete the fields, referring to the online help.

Note:

- Auto-configuration of agents is not supported for an ARS peripheral. It is greyed out on the [Advanced tab \(page 45\)](#).
- On the Advanced tab, enabling the agent state trace option can have a substantial performance impact on your system.

Skill Groups

In Unified ICM, a skill group is a collection of agents who share a common set of skills.

Skill groups are created in the Configuration Manager, and agents are assigned to them, also in the Configuration Manager.

For an ARI Deployment, you must create at least one skill group for the ARS PG. Each agent connected to the ACD/PCX must be a member of an ICM skill group to be able to log in. This is true whether or not the installation includes hard phone support.

You can configure additional skill groups as required.

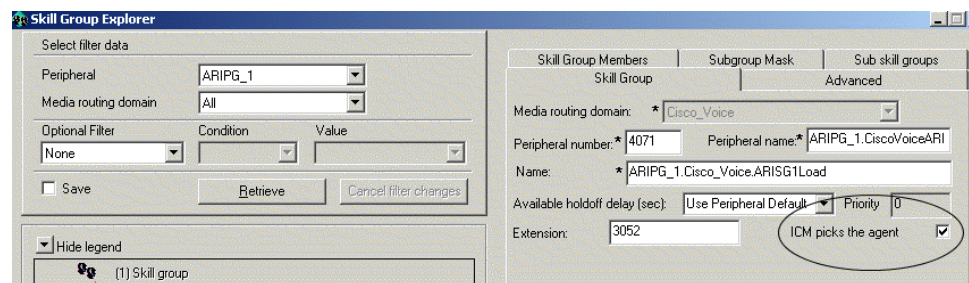
If hard phone support is used, you also need to configure a skill group on the ACD/PBX for hard phone support and to add all agents on the ACD/PBX to this skill group. The skill group extension configured on the ACD/PBX must match the skill group ID configured in Unified ICM. This ACD/PBX skill group is entered on the [Peripheral Monitor tab \(page 49\)](#) during ARS PG Configuration.

To configure a Skill Group:

1. From Configuration Manager, select **Configure ICM > Peripherals > Skill Group > Skill Group Explorer**.
2. When the Skill Group Explorer window appears, click **Add** to create a new Skill Group, or click **Retrieve** and select an existing Skill Group.

For an ARI Deployment, be sure to check **ICM picks the agent** when configuring Skill Groups:

Figure 33: Selection when Configuring Skill Groups



Configuration

“ICM picks the agent” (IPTA) means that the Central Controller is responsible for selecting the *actual agent* who will handle a request, not just the Service or Skill Group.

In traditional Unified ICME deployments, the Central Controller determines which Automated Call Distributor (ACD) has the appropriate service or skill group to handle a request and the ACD selects the actual agent to handle the call. The Central Controller pre-routes calls by targeting an ACD, and the ACD post-routes calls by selecting the agent.

In an ARI environment, the ICM Central Controller handles the post-routing of requests to agents. Choose the “ICM picks the agent” option for all skill groups that you configure for the ARS PG.

3. Complete the configuration fields on all tabs.
4. After entering the Skill Group, you can assign agents to it as Skill Group Members.

Note: Sub-skill groups are not supported for the ARS PG.

Services

A service is a type of caller need, such as Billing or Technical Support. In a traditional TDM PG environment, Services and Service Members are configured to map to applications on the ACD (such as VDN on the Avaya or Applications on the Aspect) so that the Unified ICM can report on call treatment at the ACD.

Service and Service Members are not required for ARI deployments using the ARS PG.

In an ARI deployment, Call Types with the associated script provide call treatment. WebView Peripheral Service reports are not supported. Use Call Type reports instead.

Refer to the *Reporting Guide for Cisco IPCC Enterprise & Hosted Editions* for information on planning for VRU Application Reporting.

Network Trunk Groups and Trunk Groups

For an ARI Deployment, Network trunk groups and trunk groups are not required for agent routing.

However, they need to be defined to support using Translation Routes to move the call to the ARS PG, specifically:

- for translation routing to route points within the ACD/PBX used as an IVR, and
- where the Translation Route Rule Type is used for Agent Targeting Rules

Using the Translation Route to VRU node in the Script Editor requires you to define a network trunk group and trunk group.

Configuring network trunk groups and trunk groups for the ARS PG is the same as for any other PG.

In an ARI deployment, WebView Trunk and Trunk Group reports are not supported.

Dialed Numbers

The dialed number is the number that the caller dials to initiate the call and identifies the Unified ICM routing script that should be run. Dialed numbers also need to be set up for ring on no answer, dialed number plan entries, and for Supervisor/emergency calls.

Dialed numbers are used to represent entry points on the ACD/PBX related to new calls.

Ultimately, dialed numbers equate to a VDN on the Avaya ACD/PBX. Dialed numbers are configured for the VDN(s) on the Avaya ACD/PBX that will cause a New Call message to be sent to the PIM. The Dialed Number associated with a new call will cause ICM to run a particular routing script.

The Dialed Number configured in ICM must match the VDN configured on the Avaya ACD/PBX that is responsible for handling new calls.

Device Targets

Configure Device Targets for an ARS PG as you do for IPCC.

For an ARI Deployment, if you use Agent Targeting Rules, there is no need to configure Device Targets.

If you do not use Agent Targeting Rules, you need to define Device Targets for the hard phones so that Unified ICM can route calls to agent.

If you define Device Targets for an ARS PG, for the configuration parameter, enter `/devType CiscoPhone /dn xxxxx /monitor <peripheral id of ARS Peripheral> /hardPhone 2`

For example: `/DEVTYPE CiscoPhone /DN 1000 /EXT 1000 /MONITOR 5000 /HARDPHONE 2`

If you do not require hard phone synchronization, enter `/DEVTYPE CiscoPhone /DN 1000 /EXT 1000 /MONITOR 5000`

Translation Routes

Configure Translation Routes if you have selected Rules Method and if you have selected Translation Route as the Rules Type.

Translation routes are also necessary for moving calls to and from the ACD/PBX and another PG.

How ECC variables are delivered to the ARS PG with the call.

Configuration

In traditional Unified ICM, customers required a "Translation Route" to deliver all the Call Context Data (ECC variables included) to the TDM PG.

With the introduction of an ARS PG, there is no need to do this. The Call Context is always available at the ARS PG when the call is delivered to the Agent.

However, if a call is queued at an external VRU that is connected to Unified ICM through a VRU PG, a Translation Route is needed to move the call from ARS PG to the VRU PG. This assures that the call context variables are available on the Agent Desktop when the call is delivered to the Agent.

Configure Translation Routes for an ARS PG as you do for IPCC.



Chapter 4

Queuing, Routing, and Reporting with an ARI Deployment

Queuing

Queued calls are calls that are being held at Queue Points at a Voice Response Unit (VRU) until an agent is available.

Queue Points allow the Unified ICM Router to direct calls to a VRU for call treatment prior to selecting a resource, or while waiting for a resource to become available.

The absence of an ACD makes Queue Points a necessity in an ARI configuration—there *is* no ACD to queue the calls. Queue Point functionality replaces the queuing and call treatment capability provided by an ACD.

All queues are Enterprise Queues to a Queue Point VRU, controlled by Unified ICM using the Service Control Interface (SCI).

The Service Control Interface (SCI):

- allows the Unified ICM Router to send call treatment instructions to the VRU under the control of an ICM Routing Script

(For example, the ICM Script instructs the VRU to play announcements, play music, collect digits, and eventually redirect the call to a location selected by the Router.

- allows the VRU to make use of the ICM's call routing function to select the target for a call being transferred.
- allows the PG to collect data from a VRU for use in call routing, real time monitoring, and historical reporting.

The Queue Point VRU (that is, a VRU serving as a Queue Point) may reside within the telephone **network**. If supported by the ACD/PBX, the Queue Point can also be **local** to the PBX/ACD as a [Virtual VRU \(page 23\)](#)

- **Network Queuing:**the call is queued at a VRU that is connected to Unified ICM through a PG other than the ARS PG; for example, it is queued at a VRU that is connected to Unified ICM by a VRU PG.

A call queued at a network queue point has an established SCI dialog with ICM. ICM eventually redirects the call to an available agent. ICM has control of the call while in the network queue.

- **Local Queuing:** the call is queued at Virtual VRU that resides within the ACD/PBX.

Although traditional TDM ACD queuing methods do not allow the call to be externally controlled, the ARS PG employs a methodology that 'parks' the call on the Virtual VRU at the ACD/PBX and uses post routing with extended wait times.

This 'Media Parking' queuing functionality is incorporated into the ARS PG and is also controlled by the Cisco Service Control Interface (SCI) model.

Even when you intend to use only network queuing, you need to [configure a Network VRU for the ARI peripheral \(page 39\)](#).

In an ARI deployment, therefore, ICM retains control of the call with both Network and Local queuing. This ICM control is made possible by the **Service Control Interface (SCI)** protocol.

See Also

[The Voice Response Unit \(VRU\) on page 21](#)

Routing

The Unified ICM Router is notified by the network (pre-route case) or the ARS PG (post-route case) that an incoming call has arrived.

Just as for a TDM PG, the ARS PG reports to the Unified ICM Router the current state of the agents assigned to the ACD/PBX peripheral. Based on this data, the Router invokes the routing [script \(page 61\)](#) based on the Dialed Number, Caller Entered Digits and Calling Line ID.

These three parameters classify a call into a particular "Call Type" which in turn enables the Router to run a scheduled ICM script corresponding to the Call type. The Agent is picked by the Unified ICM Router based on the availability of the agent, the data for which is sent from the ARS PG to the Router.

Scripts are user-defined and must be configured prior to routing.

In the event an agent resource is not available, or if the customer must be prompted to determine where to send the call, the Script sends the call to a Queue Point.

Pre-routing, post-routing, and translation routing are supported for the ARI deployment in the same manner as they are supported in a traditional deployment.

For traditional ACDs, Unified ICM routes are a collection of peripheral targets.

In an ARI environment, calls can be routed to device targets and to peripheral targets. Device targets indicate individual agents to whom calls can be routed. Peripheral targets are used for Translation Routing and for post-route points.

In an ARI environment, calls can be routed:

- directly to an agent phone, using Device Targets or Agent Targeting Rules
- to a Queue Point on a Virtual VRU and then to an agent
- to a network VRU and then to an agent

Device Targets and Agent Targeting Rules

For Unified ICM to send calls to agents on the ACD/PBX, you must configure routes to route directly to the agent phones.

There are two ways to do this. One is to use Device Targets and the other is to use Agent Targeting Rules.

The method you use depends on the Agent Targeting Mode indicated in the [Advanced tab of the PG Configuration \(page 45\)](#):

- If you selected **Device Targets Preferred** for the Agent Targeting Mode, you must configure Device Targets.
- If you selected **Rules Preferred** for the Agent Targeting Mode, you must configure Agent Targeting Rules.

Device Targets

Device targets are configured to identify devices that can be targeted by the ICM Router to deliver a call to agent at the ACD/PBX. An agent is dynamically associated to the device target at the time the he or she logs in.

A Device Target is a separately addressable device. It is not exclusively owned by a particular agent or associated with a particular peripheral. Device Targets are dynamically associated with agents for the duration of a given log-on session.

You must configure a Device Target for each independently addressable telephony device. This can be a long process requiring hundreds of unique configurations.

See also the section on [configuring Device Targets \(page 55\)](#).

Agent Targeting Rules

Routing

To target agents directly without configuring DeviceTargets, you need to create Translation Routes and Agent Targeting Rules.

Agent Targeting Rules eliminate the need to create hundreds of device targets.

When Agent Targeting Rules are used, agent extensions are in the Peripheral Monitor tab in the ARS Peripheral.

Caution: In this case, do not configure Device Targets for these extensions. Extensions must be configured either as Device Targets or as an entry on the Peripheral Monitor screen, but not in both places.

See also the sections on the [Peripheral Monitor tab \(page 48\)](#) and on [Configuring Agent Targeting Rules \(page 49\)](#)

Pre-Routing

Pre-routing enables call routing decisions to be made prior to a call being terminated at a call center.

In an ARI deployment, calls are routed directly to an agent or routed to a queue point if an agent is not available.

Pre-routing calls directly to agents requires that routes have been configured to agent phones. See [Device Targets and Agent Targeting Rules \(page 59\)](#).

Post Routing

The Post Routing feature allows the ACD/PBX to request a route to a new destination from the Router.

The Router then makes a routing decision based on real-time enterprise wide resource availability. This allows previously terminated calls to be redirected to a new optimal location.

The new location could be on the same ACD/PBX, or the call could be sent to an alternate location.

Translation Routing

Translation routing ensures that the association between a call and its related data is maintained throughout the life of the call.

With traditional ACDs, translation routes allow the Unified ICM to pass data along with a call even when the call is delivered to a generic resource at an ACD, such as a queue or an application.

In an ARI deployment, translation routing is used to route calls that are

- sent *to* an application on the ARS PG or queued at the ARS PG using the Virtual VRU functionality *from* another PG or Routing Client
- sent *from* the ARS PG to another ICM PG.
- routed by Agent Targeting Rules where the Rule Type is Translation Route

Translation routes are not required when a call is transferred between agents within the same ACD/PBX.

See the Cisco White Paper on [Working with Translation Routes](http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1001/prod_technical_reference09186a0080134922.html) (http://www.cisco.com/en/US/partner/products/sw/custcosw/ps1001/prod_technical_reference09186a0080134922.html)

Scripting

Unified ICM software uses routing scripts to determine the best destination for a call by assessing the current information extracted by the PGs regarding call center activity.

When notified by the network (pre-route case) or the ARS PG (post-route case) that an incoming call has arrived, the Router invokes the appropriate routing script to select a destination agent, based on the real-time data provided by the ARS PG.

Once an agent has been selected, the ICM Router instructs the network to deliver the call to the selected agent and notifies the target ARS PG that a call is on the way.

The ARS PG instructs the CTI Server to notify the agent desktop of the incoming call, which allows an appropriate screen pop.

The PIM process running on the target ARS PG detects the arrival of the routed call. This event is communicated by the PIM to the OPC process, which provides feedback to the Router via an agent state update, as well as notification to the CTI Server.

Routing scripts are a representation of your business rules.

- You can create a specific set of scripts to be executed for each Call Type, such as Sales or Support. For more granular reports, you might want to create multiple scripts; for example, you might create a script for initial call classification and also create scripts that route calls that are sent to particular services or skill groups on different ACDs.
- You can schedule different scripts to be used at different times of day or different days of the week and year for each Call Type.
- Use ICM dialed numbers to direct calls to scripts that handle transfers.
- The Unified ICM Router scripting language provides a scriptwriter with much more power than is typically afforded a scriptwriter on an ACD. The customer can change the agent

Using WebView with your ARI Deployment

selection algorithm simply by modifying the Unified ICM Script associated with the given Call Type.

- Translation routing scripts are used to route calls to the ARS PG by another PG.

In an ARI deployment, scripting on the PBX/ACD is limited to scripts for the Virtual VRU. See the *System Manager Guide Supplement for Avaya ARS PG*.

See the *ICM Scripting and Media Routing Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for full details on scripting.

Using WebView with your ARI Deployment

The reporting statistics gathered for Unified ICM deployments with ARI are similar to the statistics gather from Unified Contact Center (IPCC).

When you generate reports for the ARS PG and for the agents, skill groups, and other entities associated with it, you need to select the *IPCC* report templates.

Figure 34: WebView Template Selection

This wizard helps you develop an ICM and/or IPCC report.

Select one template to create your report, then click Next.

Select the type of templates (Templates can appear in multiple types).

ICM Templates IPCC Templates

IPCC reporting templates are supported for an ARI deployment, with the exception of the Peripheral Service and the Trunk and Network Trunk Group templates.

If you are familiar with a traditional ICM environment and with using the WebView ICM report templates, you might benefit from familiarizing yourself with IPCC reporting.

See the *Reporting Guide for Cisco IPCC Enterprise & Hosted Editions* for details on IPCC Reporting.

The *Reporting Guide for Cisco IPCC Enterprise & Hosted Editions* includes a discussion of reporting in a hybrid deployment.

See also the section [Configuring for Reporting in an ARI Deployment \(page 51\)](#).



Chapter 5

Desktops and Call Control

About Computer Telephony Integration

The ARS PG relays information to Unified ICM about the agent desktop—such as telephony operations and agent state—by way of a CTI link.

This CTI link is made available by the ICM CTI Object Server process, which is a server-based solution for deploying CTI applications. The CTI Server and CTI OS are installed on the ARS PG server, co-located with the ARS PG.

The CTI interface provides a CSTA message model that allows desktop clients and business applications to receive unsolicited call and agent state transition events. In addition to providing an unsolicited event feed, the CTI Server provides the ability to perform call control functions (such as transfers) from the agent and supervisor desktop.

In a direct desktop application environment, call event information is delivered to the targeted desktop when the call is delivered. CTI Server reports call events and agent work state changes to the application as they occur through each stage of the call flow—from the moment a call arrives at the answering resource (the ACD/PBX) until the caller hangs up.

Agent Phones

Agents can log in and perform call control using the desktop softphones included with the CTI OS³ and also by using "hard phones" (the standard agent handsets supported by the ACD/PBX).

3) CTI OS also provides CTI OS Active X Controls that allow you to design a user interface that will closely resemble the appearance of an ACD telephone set.

Softphone

Although calls can be placed by either the hard phone or softphone, placing calls by the softphone has the advantage of allowing Unified ICM routing scripts to be used to determine the best destination of the call based on the current condition of the Enterprise call center.

Softphones may be preferred or even required; for example, when reason codes are mandated by the Agent Desktop settings.

The agent and supervisor desktops include a fully-functional softphones that enables telephony functions from the desktop.

Buttons on the softphones for state and call control are similar on both agent and supervisor desktop softphones.

Note: For more information on Softphones Controls, Softphones, and Agent state, see the *CTI OS Developer's Guide*.

Hard Phones

The ARI deployment supports function keys on hard phones as backup in situations of server or network failure.

For this release, supported "hardphones" are Avaya phones connected to the Avaya switch.

Using the hard phone, an agent can answer a call, place a caller on Hold, retrieve the call, transfer and conference the call, and end the call.

Since all calls are routed by Unified ICM, the **agent state changes** supported on the hard phone are the keys for **Login, Logout, Auto In, and Aux In**.

Note: The access codes must be programmed into the programmable buttons on the hard phones. **DO NOT enter the codes manually.** Manual entry is not supported.

When agents press the buttons for Log In, Log Out, Auto In, and Aux In, those states are reflected in WebView reports and on the softphone.

Note: The exception to this is Log In. It is reflected in the reports but not on the softphone.

Call control is also synchronized between the hard phone and the softphone.

The Agent State changes recorded and synchronized from the hardphone functions are as follows:

- Unknown to Not Ready at Login
- Ready at Auto In
- Not Ready at Aux In
- Logged Out at Logout

An agent skill group/hunt group must be set up on the ACD/PBX so agents can log in using their hard phone. Agents also need to be defined on the ACD/PBX to have the same agent ID as those used in the ICM configuration. These agents are then assigned to the ACD/PBX skill group.

If hard phone support is required, there might be ARS-specific requirements for agent ID and password at login. Refer to the appropriate *System Manager Guide Supplement*.

Synchronization

When the hard phone and softphone are synchronized, they look like a single device to Unified ICM and the user.

Agents must log in using their softphone, even after logging in through their hard phone. This is required so that the softphone reflects the Agent States and Call control. There is no way to know which Client (or SoftPhone) machine is being used by the Agent through a hardphone "log in". So the Softphone cannot show agent as logged in automatically.

Synchronization is performed for agent state activities and for call related actions. Agent state activities include logging in, changing state, and logging out. Call related actions include answering, transferring, conferencing, holding, and releasing calls.

Hard phone/softphone synchronization is performed through special configuration in both Unified ICM and the ACD/PBX. ICM needs to know which hard phone devices need to be synchronized.

This is done with a configuration parameter in either the Peripheral Monitor tab or the Device Target configuration.

- If you use [Agent Targeting Rules \(page 49\)](#), you must configure the [Peripheral Monitor tab \(page 48\)](#) for Hardphone Support Level 2 to ensure synchronization between the agent's softphone and the agent's teleset device.
- If you are not using Agent Targeting Rules, you must add each hard phone device in the [Device Target \(page 55\)](#) configuration: `/monitor [peripheral ID] /HARDPHONE 2.`

Desktops and Call Control

Topics in this section include:

- [The Agent Desktop \(page 66\)](#)
- [The Supervisor Desktop \(page 66\)](#)
- [Desktop Differences \(page 67\)](#)

The Agent Desktop

An Agent Desktop is a Windows-based desktop application that provides an interface to enable the agent to perform agent state control and call control.

Agent Desktops are a required component of an ARI deployment.

The following agent desktop functionality is supported for the ARI Deployment:

- Login
- Logout
- Make calls
- Answer calls
- Transfer calls to another agent or to the Supervisor
- Place calls on Hold
- Conference calls to other agent(s)
- Conference the Supervisor into the call
- Request Supervisor assistance
- Reconnect back to the caller after receiving Supervisor assistance
- Release (hang up) a call.

The Supervisor Desktop

The Supervisor Desktop provides all of the functionality of the Softphone, with additional functions for monitoring and managing Agent Team members.

In addition to the softphone, the supervisor desktop also has:

- A Team Real-Time Status window that provides supervisors with information about the current state of agents who are part of their team.
- A CTI Statistics that displays individual statistics for the agent logged onto the phone, as well as statistics for the supervisor who is currently logged on and for the skill groups to which the supervisor and the supervisor's team belongs.

Note: Silent Monitoring is not supported.

Supervisor features include the ability to respond to an agent request for assistance, the ability to barge in to an existing ACD call, and the ability to remove the agent from the call once he has barged in (intercept).

The following supervisor desktop functionality is supported for the ARI Deployment:

- Change the agent state of a supervised agent to Logout and Ready
- Perform call monitoring features (barge in and intercept)
- Support emergency and supervisor assist calls.
- Allow exchange of text messages between the supervisor and one of the agent team members or all agent team members (chat).
- Control their own states for receiving assist calls.

Desktop Differences

In an ARI deployment, the Agent Desktop behavior is that of Unified Contact Center and not of Unified ICM.

Some differences you see when moving from a TDM PG to and ARS PG are the following:

- Agents cannot make calls from their softphones when they are in the Ready state. They must be in Not Ready state to initiate a call
- There is no dropdoen menu to select Work Mode (Unspecified, Auto In, or Manual). The agent's work mode is controlled by the [Agent Desk Settings configuration \(page 40\)](#).

If you move from a traditional PG to the ARS PG, you might need to train contact center agents on the changed agent desktop behavior.

Agent States

The agent state model determines call delivery to agents and defines the valid state transitions an agent may initiate. The agent state model for an ARI deployment is based on the model created for Unified Contact Center. Existing TDM PBXs with traditional ACD software may have existing Agent State Models that differ from this model.

These are the agent state values that are relayed to the Unified ICM Router by the ARS PG.

State	Description
Login	The agent has logged on to the ACD/PGX. This state does not necessarily indicate that the agent is ready to accept calls.
Logout	The agent has logged out of the ACD/PBX and cannot accept any additional calls.

Agent States

State	Description
NotReady	The agent is unavailable for any call work.
Available	The agent is ready to accept a call.
Talking	The agent is currently talking on a call.
WorkNotReady	The agent is performing wrapup work and will enter NotReady state when the wrapup is complete.
WorkReady	The agent is performing wrapup work and will enter Ready state when the wrapup is complete.
BusyOther	The agent is busy performing a task (is Talking, WorkReady, Reserved, or Hold state in another SkillGroup).
Reserved	The agent is reserved for a call that will arrive at the ACD/PBX shortly.
Unknown	The agent state is currently unknown.
Hold	The agent currently has all calls on hold.

Changing Agent State from the Desktop

Desktop agent state controls include:

- Login/Logout
- Ready/NotReady

Depending on the [Agent Desk Setting configuration \(page 40\)](#), NotReady might require a Reason Code.

- Wrap up

Depending on the [Agent Desk Setting configuration \(page 40\)](#), wrapup might be required, optional, or not allowed. The agent state that is communicated to Unified ICM depends on the configuration.

Notes on Agent State Transitions

- **Login**

At log in, agents are put in a “Not Ready” state and cannot receive routed calls until they click the Ready button.

- **Ready/Available:** When the agent clicks the “Ready” button, the agent enters the Available state and can receive routed calls
- An agent in the Available state cannot make a call (the line buttons are dimmed). The agent must click the “Not Ready” button and become unavailable before being allowed to make a call.

An agent in the Available state cannot log out (the logout button is dimmed). The agent must click the “Not Ready” button and become unavailable before being allowed to logout.

- **Not Ready:** Agents must be in a “Not Ready” state in order to make a call.

Transitions to the Not Ready state might be disallowed if the Router has sent a call to the agent within the last 10 seconds.

- **WorkReady and WorkNotReady:** The difference between Work Ready and Work Not Ready is that Work Ready transitions to Ready, and Work Not Ready transitions to Not Ready.

While on a call, if an agent clicks on the "Make Ready" button and then clicks Wrap up, the state transitions are as Talking -> Work Ready -> Ready.

While on a call, if an agent clicks on the "Make Not Ready" button and then clicks Wrapup, the state transitions are as Talking -> Work Not Ready -> Not Ready

- **Agent states for receiving a routed call:** Talking

Notes:

1. If certain options (such as Idle Reason or Logout Reason) are checked on the Agent Desk Settings, dialog boxes display prompting for a reason. Transition cannot occur until the agent enters a reason. If the agent does not enter a reason and the Work Mode timer expires, the agent is transitioned to the Ready state and the dialog closes.
2. When the agent is talking and agent state buttons are enabled, once the agent presses the Ready, Not Ready, or Wrap buttons, that button becomes disabled. If the agent then presses a subsequent agent state button, the former button becomes enabled and the most recently pressed button becomes disabled. The last button pressed before the call ends defines the next agent state.

Index

- ACD/PBX....[11](#), [21](#)
 - agent skill groups....[52](#), [53](#)
 - configuring....[38](#)
 - currently supported for ARI....[12](#)
- Active Directory....[15](#)
- Administrative Workstation (AW)....[20](#), [29](#), [38](#)
- Advanced tab (ARS PG)....[45](#)
- Agent Desk Settings....[40](#)
- agent desktop....[66](#)
 - changing states....[68](#)
- Agent Distribution tab (ARS PG)....[46](#)
- agent-level routing....[24](#)
- Agent Routing Integration (see ARI)....[11](#)
- Agent Routing Services
 - client type....[31](#)
- agents
 - configuring....[52](#)
- agent states
 - and Agent Desk Setting configuration....[40](#)
 - and hard phones....[64](#)
 - changing at desktop....[68](#)
 - transitions....[68](#)
- Agent Targeting Mode....[45](#)
- Agent Targeting Rules....[13](#), [59](#)
 - configuring....[49](#)
- ARI
 - deployment models....[24](#)
 - overview....[11](#)
 - reporting....[12](#)
 - supported features....[13](#)
 - unsupported features....[14](#)
- ARS Gateway....[19](#), [27](#)
 - ARS PG....[11](#), [28](#)
 - ARS Gateway....[19](#)
 - configuring....[29](#), [42](#)
 - currently supported....[12](#)
 - installing....[30](#)
 - in the Unified ICM enviroment....[18](#)
 - OPC....[19](#)
- ARS PG server....[27](#)
 - preparing for the ARS PG....[28](#)
- Central Controller....[17](#)
- Central Database....[17](#)
- Cisco product name changes....[1](#)
- Configuration Manager....[37](#), [38](#)
 - configuring
 - ACD/PBX....[38](#)
 - Agent Desk Settings....[40](#)
 - agents....[52](#)
 - Agent Targeting Rules....[49](#)
 - ARS PG....[29](#), [42](#)
 - ARS PG Advanced tab....[45](#)
 - ARS PG Agent Distribution tab[46](#)
 - ARS PG Default Route tab....[47](#)
 - ARS PG Peripheral Monitor tab....[48](#)
 - ARS PG Peripheral tab....[43](#)
 - ARS PG Routing Client tab....[46](#)
 - ARS PIM....[32](#)
 - Device Targets....[55](#)
 - hard phone extensions....[49](#)
 - network VRU....[39](#)
 - reporting....[51](#)
 - skill groups....[53](#)
 - translation Routes....[55](#)
- cradle-to-grave tracking....[13](#)
- CTI OS....[21](#), [27](#)
 - installing....[35](#)

- CTI Server....[20](#), [27](#), [29](#), [63](#)
 - installing....[28](#)
- Default Route tab (ARS PG)....[47](#)
- desktops....[21](#)
 - agent....[66](#)
 - behavior in ARI deployment....[67](#)
 - configuring Agent Desk Settings....[40](#)
 - installing....[36](#)
 - supervisor....[66](#)
- Device Targets....[45](#), [59](#)
- Device Targets
 - configuring....[55](#)
- dialed numbers....[55](#)
- ECC variables....[55](#)
- enable agent reporting....[46](#)
- enterprise routing....[24](#)
- fault tolerance....[16](#)
- feature access codes....[64](#)
- hard phone
 - extensions....[48](#), [53](#)
 - synchronization....[65](#)
- hard phones....[63](#)
 - access codes....[64](#)
 - agent states....[64](#)
 - supported....[64](#)
- hybrid deployment....[24](#)
- installing
 - ARS PG....[30](#)
 - CTI OS....[35](#)
 - CTI Server....[28](#)
 - desktops....[36](#)
 - Release 7.2(1)....[29](#)
- internal port switching....[21](#)
- ISAGI....[19](#), [23](#)
- IVR....[21](#)
 - local setup....[28](#)
- Logger....[17](#)
- media setup....[28](#)
- Microsoft Windows....[15](#)
- multi-media integration....[14](#)
- Network trunk groups....[54](#)
- network VRU....[22](#), [24](#), [45](#), [58](#)
 - configuring....[39](#)
- OPC....[18](#)
 - for ARS PG....[19](#), [27](#)
- operating system....[15](#)
- Outbound Option....[14](#)
- Peripheral Gateway (see PG)....[17](#)
- Peripheral Monitor tab (ARS PG)....[48](#)
- Peripheral tab (ARS PG)....[43](#)
- PG....[17](#)
- phone synchronization....[49](#)
- PIM....[18](#)
 - for ARS, configuring....[32](#)
 - for ARS PG....[27](#)
- post-routing....[60](#)
- pre-routing....[60](#)
- queue points....[57](#), [58](#)
- queuing....[12](#), [57](#)
- Release 7.2(1)
 - ARS PG....[28](#)
- reporting....[12](#), [62](#)
 - configuring....[51](#)
 - enable agent reporting....[46](#)
 - templates....[51](#)
 - unsupported reports....[14](#)
- RONA....[14](#), [40](#)
- Router....[17](#)
- routing....[12](#), [58](#)
 - agent-level....[24](#)

- enterprise....[24](#)
- hybrid....[24](#)
- pre-routing....[60](#)
- scripts....[61](#)
- Routing Client tab (ARS PG)....[46](#)
- SCI....[23](#), [57](#)
- scripts....[61](#)
- server platforms....[16](#)
- Service Control Interface (see SCI)....[21](#)
- services....[54](#)
- silent monitoring....[14](#)
- skill groups
 - ACD/PBX....[48](#), [52](#), [53](#)
 - configuring....[53](#)
- softphone
 - synchronization....[65](#)
- softphones....[63](#)
- sub-skill groups....[14](#), [46](#), [54](#)
- supervisor desktop....[66](#)
- synchronization....[49](#)
- system architecture
 - Administrative Workstation....[20](#)
 - Central Controller....[16](#)
 - Logger....[17](#)
- TDM ACD
 - retaining existing hardware....[12](#)
- telephone network....[16](#), [21](#)
- translation routes....[50](#)
- translation routes
 - configuring....[55](#)
- Type 9 VRU....[39](#)
- Virtual VRU (VVRU)
 - scripts....[21](#), [23](#), [48](#)
- VRU....[21](#)
- WebView....[51](#), [62](#)