Avaya Interaction Center 7.3.4 Service Pack Release Notes

Release 7.3.4

December 2015

that hosts a software application to be accessed by multiple users. "**Instance**" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("**VM**") or similar deployment.

License types

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User," means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software
"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products," or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

"**Third Party Components**" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation
For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

The Avaya Interaction Center 7.3.4 Service Pack (SP) Release Notes provides information on installation and configuration of IC 7.3.4 SP. You should also refer this document either for fresh IC installation or upgrading of existing IC installations (IC 7.3 RTM or IC 7.3.x SP/FP) to 7.3.4 SP.

Intended audience

This document is for the customers using Avaya Interaction Center. You should use this document for upgrading the existing IC installation to SP 7.3.4.

The audience for this guide includes:

- Application consultants

- Integration consultants

- Avaya Business Partners

- Customers

Files Changed in IC 7.3.4 Service Pack

Following is the list of files updated in IC 7.3.4 Service Pack Release

- Avaya Interaction Center and Avaya Operational Analyst Overview and Specification

- IC Installation Planning and Prerequisites

- IC Installation and Configuration

- IC Administration Guide

- Agent Data Unit Server Programmer Guide

- Avaya IC for Siebel 8 Integration Guide

- File list with modification time stamp and version numbers for AIC 7.3.x

- Avaya IC/OA Port Matrix

Related resources

Documentation

For updated documentation, product support notices, and service pack information, visit the Avaya Support Center website at http://support.avaya.com.

Title	Description
Avaya Interaction Center and Avaya Operational Analyst Overview and Specification	This document describes tested Interaction Center (IC) and Operational Analyst (OA) characteristics and capabilities, including feature descriptions, interoperability, performance specifications, security, and licensing requirements.
IC Integration with VP / IR	The purpose of this guide is to provide detailed information about Avaya Interaction Center (IC) integration with Avaya Aura® Experience Portal (EP) / Avaya Voice Portal (VP) / Avaya Interactive Response (IR).This guide is intended for Application consultants, Integration consultants, Avaya Business Partners, and customers.
Installation and Configuration	
IC Installation Planning and Prerequisites	The purpose of this guide is to provide detailed information about the planning and third-party software required to deploy an Avaya Interaction Center, Release 7.3.x system.
IC Installation and Configuration	The purpose of this guide is to provide detailed information about how to install and configure an out-of-the-box Avaya Interaction Center Release 7.3.x.
Using Config Accelerator	The purpose of this guide is to provide detailed information about how to use Config Accelerator for simplifying and accelerating the configuration process of Avaya Interaction Center 7.3.x.
IC Database Designer Application Reference	The purpose of this guide is to provide detailed information about Avaya Interaction Center (IC).This

Title	Description
	guide describes the prerequisites for installing and configuring Avaya IC
Agent Web Client Customization	The purpose of this guide is to provide detailed information about how to customize Avaya Agent Web Client.
IC Business Advocate Configuration and Administration	The purpose of this guide is to provide detailed information about Administration Avaya Interaction Center (IC) 7.3.x. This guide describes the administration and configuration of Avaya Business Advocate.
Administration	
IC Administration Guide	The purpose of this guide is to provide detailed information about Avaya Interaction Center (Avaya IC). This guide describes domain and server administration using Avaya IC Manager.
Events and Alarms	
IC Alarms Guide	The purpose of this guide is to provide detailed information about Avaya Interaction Center alarms.
Using	
Agent User Guide	The purpose of this guide is to provide agent-related information about Avaya Interaction Center Agent.
Avaya Agent Web Client	The purpose of this guide is to provide the information about |Avaya Agent Web Client.
Reference	
IC Media Workflow Reference	The purpose of this guide is to provide detailed information about the blocks you can use with media workflows and other reference information to help you understand and customize media workflows for Avaya Interaction Center Release 7.3.x.
Agent Script Workflow Reference	The purpose of this guide is to provide detailed information about the blocks you can use with agent script workflows and other reference information to help you understand and create agent script workflows for Avaya Interaction Center Release 7.3.x.
IC Workflow API Reference	The purpose of this guide is to provide information about the extensions and methods specific to the

Title	Description
	Application Programming Interface (API) for workflow blocks in Avaya Interaction Center Release 7.3.x.
Programming	
IC Client SDK Programmer Guide	The purpose of this guide is to provide detailed information about the Client Software Development Kit (Client SDK) for Avaya Interaction Center Release 7.3.x.
IC Client and Server Programmer Design Guide	The purpose of this guide is to provide detailed information about Avaya Interaction Center (Avaya IC). The purpose of this guide is also to provide an overview of the Avaya IC ORB Toolkit, and a list of components in the Avaya IC product set.
Agent Data Unit Server Programmer Guide	The purpose of this guide is to provide detailed information about configuring and managing the Agent Data Unit (ADU) server, which is responsible for tracking the state of agents at the contact center. This guide is intended for administrators who are authorized to configure and manage the Agent Data Unit (ADU) server.
Core Services Programmer Guide	The purpose of this guide is to provide detailed information for programming and changing the configuration of your IC Core Services. This guide is intended for those who install and configure Interaction Center.
Electronic Data Unit Server Programmer Guide	The purpose of this guide is to provide detailed information about the Electronic Data Unit (EDU) server, which was previously named the Voice Data Unit (VDU) server, the EDU server configuration, the alarms, and the event monitoring. This guide is intended for administrators who are authorized to configure and manage the Electronic Data Unit (EDU) server.
IC Telephony Connectors Programmer Guide	The purpose of this guide to describe the Avaya Telephony Connector server. This guide is intended for those who use Interaction Center. You should use this guide as an information source for programming and changing the configuration of your Telephony Connector server.

Comments on this document? infodev@avaya.com

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course title in the Search field and click Go to search for the course.

Course code	Course title
ATC01175WEN	IC and OA Overview
ATC01176IEN	Interaction Center Administration and Configuration
AUCC100010695	IC-Siebel Integration
ATC100011017	IC Siebel Integration, Installation and Troubleshooting

Avaya Mentor videos

Avaya Mentor videos are available to provide technical content on how to install, configure, and troubleshoot Avaya products.

Videos are available on the Avaya support site, listed under the video document type, and on the Avaya-run channel on YouTube.

To find videos on the Avaya support site, select the product name, and check the videos check box to see a list of available videos.

Note: Videos are not available for all products.

To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:

- Enter a key word or key words in the Search Channel to search for a specific product or topic.

- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: Overview

The Avaya Interaction Center (IC) software updates are distributed in service packs. The Avaya Interaction Center (IC) 7.3.4 Service Pack (SP) is the fourth release on top of IC 7.3. The SP is cumulative release which also includes all the fixes from IC 7.3.1 SP, IC 7.3.2 FP and IC 7.3.3 FP. This software update includes fixes and features that are not included in the original release of IC 7.3.

Avaya recommends that all IC 7.3 customers update to the 7.3.4 SP level to ensure you have a complete set of fixes. IC 7.3.4 does not include a redelivery of the entire IC product. The IC 7.3.4 SP can be directly installed on IC 7.3. Follow the instructions in the Release Notes when installing and configuring the IC 7.3.4 Service Pack. Information, such as known defects and defects fixed in this release, and solutions for some known issues, which might not necessarily be included in the standard IC 7.3 documentation, are included in a separate document named List of Fixed Issues, Improvements, Known Issues, and Troubleshooting for Avaya Interaction Center 7.3. Similarly, the files shipped with SPs and the versions are included in the document titled as "Feature Pack File List IC 73x.pdf" with modification time stamp and version numbers for Avaya Interaction Center 7.3. All these documents are available for download at http://support.avaya.com.

The existing features in Interaction Center Release 7.3, 7.3.1, 7.3.2, 7.3.3 continue to be in use, unless mentioned otherwise in the Release Notes.

Note: IBM AIX is only supported on Interaction Center Release 7.3, 7.3.1, and 7.3.2. For more information see the Supported Server Operating Systems section in the *Avaya IC Installation Planning and Prerequisites Guide*. All the information related to IBM AIX and IBM DB2 is only applicable to Interaction Center Release 7.3, 7.3.1, and 7.3.2.

Refer to the section, Product Support Information, in this Release Notes for information that was published as PSNs.

The Release Notes provides detailed installation and configuration information. The Installation Tool provided with this SP easily installs all the fixes in the IC 7.3.4 SP.

For additional IC 7.3 documentation information, see:

- Interaction Center (IC) 7.3 Product Documentation

- Interaction Center (IC) 7.3 Release Notes

- Avaya IC for Siebel 8 Integration Guide

Following tables lists IC compatibility with different platforms/softwares.

Supported Server Operating System

Platforms	IC 7.3	IC 7.3.1	IC 7.3.2	IC 7.3.3	IC 7.3.4
Microsoft Windows					
Windows 2012 Server R2	✗	✗	✗	✓	✓
Microsoft Windows 2008 Server R2 (x64) (Enterprise Edition).	✓	✓	✓	✓	✓
IBM AIX					
IBM AIX 6.1 update 3	✓	✓	✓	✗	✗
Linux					
RHEL 6.5 (64 Bit) **Only Siebel Integration**	✗	✗	✗	✗	✓

Supported Desktop Operating System

Platforms	IC 7.3	IC 7.3.1	IC 7.3.2	IC 7.3.3	IC 7.3.4
Microsoft Windows					
Windows 10	✗	✗	✗	✗	✓
Windows 8.1	✗	✗	✗	✓	✓
Microsoft Windows 7 (32 and 64 Bit)	✓	✓	✓	✓	✓
Microsoft Windows Vista	✓	✓	✓	✗	✗
Microsoft Windows XP	✓	✓	✓	✗	✗

Supported Database Server Software

Database Server Software	IC 7.3	IC 7.3.1	IC 7.3.2	IC 7.3.3	IC 7.3.4
Microsoft SQL					
Microsoft SQL 2014	✗	✗	✗	✓	✓
Microsoft SQL 2012	✗	✗	✗	✓	✓
Microsoft SQL Server 2008 (v10.50.1600.1).	✓	✓	✓	✓	✓
Oracle					
Oracle 12.1 database	✗	✗	✗	✓	✓
IBM					
IBM DB2 9.5	✓	✓	✓	✗	✗

Supported Database Client Software

Database Client Software	IC 7.3	IC 7.3.1	IC 7.3.2	IC 7.3.3	IC 7.3.4
Oracle					
Oracle Database 11g Client Release 11.2.0.1.0	✓	✓	✓	✓	✓
Oracle Database 11g Client Release 11.2.0.4.0	✗	✗	✗	✓	✓

Supported Virtualization Software

Virtualization Software	IC 7.3	IC 7.3.1	IC 7.3.2	IC 7.3.3	IC 7.3.4
VMware VDI (HORIZON VIEW 6)	✗	✗	✗	✓	✓

Virtualization Software	IC 7.3	IC 7.3.1	IC 7.3.2	IC 7.3.3	IC 7.3.4
VMware 6.0 ESXi (WIN)	✗	✗	✗	✗	✓
VMware 5.5 ESXi (WIN)	✗	✗	✗	✓	✓
VMWare 4.1	✓	✓	✓	✓	✓
Citrix XenApp 7.5	✗	✗	✗	✓	✓
Citrix XenDesktop 7.5	✗	✗	✗	✓	✓
Citrix XenApp 6.0 on Windows 2008 R2.	✓	✓	✓	✓	✓

Supported Siebel Integration

Siebel Software	IC 7.3	IC 7.3.1	IC 7.3.2	IC 7.3.3	IC 7.3.4
Siebel 15	✗	✗	✗	✗	✓
Siebel 8.2.2.4 open UI	✗	✗	✗	✓	✓
Siebel 8.1.1.11 open UI	✗	✗	✗	✓	✓
Siebel 8.1.1.x	✓	✓	✓	✓	✓
Siebel 7.8.2.13	✓	✓	✓	✗	✗

Supported Web Server Software

Web Server Software	IC 7.3	IC 7.3.1	IC 7.3.2	IC 7.3.3	IC 7.3.4
IIS 8	✗	✗	✗	✓	✓
Hosting IC website using IIS 7.0 on Windows 2008 R2.	✓	✓	✓	✓	✓
Hosting IC website using IBM HTTP Server 7.x on AIX 6.1.	✓	✓	✓	✗	✗

Supported Browser Software

Browser Software	IC 7.3	IC 7.3.1	IC 7.3.2	IC 7.3.3	IC 7.3.4
Internet Explorer 11 (32-bit only)	✗	✗	✗	✓	✓
Internet Explorer 10 (32-bit only)	✗	✗	✓	✓	✓
Internet Explorer 9 (32-bit only)	✗	✗	✓	✓	✓
Internet Explorer 8	✓	✓	✓	✗	✗
Internet Explorer 7	✓	✓	✗	✗	✗

Note:

Microsoft Edge browser is the default browser in Microsoft Windows 10. You must only use Internet Explorer browser for IC applications.

Supported Avaya Software

Avaya Software	IC 7.3	IC 7.3.1	IC 7.3.2	IC 7.3.3	IC 7.3.4
Secured authentication using ASG (Access Security Gateway)	✗	✗	✓	✓	✓
WebLM 6.3.4 Upgrade	✗	✗	✓	✓	✓
ASG plugin on Windows 2012 for AIC	✗	✗	✗	✓	✓
AES v7.1 GRHA	✗	✗	✗	✗	✓

Supported Non-Avaya Software

Non-Avaya Software	IC 7.3	IC 7.3.1	IC 7.3.2	IC 7.3.3	IC 7.3.4
JRE 1.8.0_40 (Windows) JRE 1.7.0 (Solaris)	✗	✗	✗	✗	✓
JRE 1.6.0_45	✗	✗	✓	✓	✗
JRE 1.6.0_10	✗	✓	✗	✗	✗
Tomcat 8.0.27	✗	✗	✗	✗	✓
Tomcat 6.0.37	✗	✗	✓	✓	✗
Tomcat 6.0.14	✗	✓	✗	✗	✗
Java Mail 1.5.2	✗	✗	✗	✗	✓
Java Mail 1.4.7	✗	✗	✗	✓	✗
Ephox Editlive 9.1.0.287	✗	✗	✗	✗	✓
Ephox Editlive 9.0.0.98	✗	✗	✓	✓	✗
Ephox Editlive 7.5.2.106	✓	✓	✗	✗	✗
SIP end point support	✗	✗	✓	✓	✓

Features

Following table lists features provided by IC 7.3.x releases.

Feature	IC 7.3	IC 7.3.1	IC 7.3.2	IC 7.3.3	IC 7.3.4
Chat Features					
Options to set column width, size, and location of chat task list in IC agent.	✓	✓	✓	✓	✓
Chat Typing Status Support.	✓	✓	✓	✓	✓
Web chat UI and API	✗	✗	✓	✓	✓
Security Enhancements	✗	✗	✓	✓	✓

Feature	IC 7.3	IC 7.3.1	IC 7.3.2	IC 7.3.3	IC 7.3.4
Automatic public chat disconnect when caller inactivity crosses the disconnect interval set in ICM	✗	✗	✓	✓	✓
Tool to configure and deploy CSPortal Client or Public Website on IIS	✗	✗	✗	✓	✓
Maintaining existing AIC R7.3.2 FP chat feature and functionalities	✗	✗	✗	✓	✓
EWT for web based customers (with IC BA only)	✗	✗	✗	✓	✓
Support for chat session across multiple tabs in CSPortal.	✗	✗	✗	✓	✓
Save chat transcripts in txt format in CSPortal	✗	✗	✗	✓	✓
Survey page in CSPortal	✗	✗	✗	✓	✓
Support for customer account in CSPortal	✗	✗	✗	✓	✓
Enhanced chat transcript search & sort for agents & supervisors	✗	✗	✗	✓	✓
Reset chat timeout duration when customer responds back to agent	✗	✗	✗	✓	✓
Set schedule call back question char max length (nvchar) to 999 in database	✗	✗	✗	✓	✓
All chat api to be rest based	✗	✗	✗	✓	✓
Chat properties localized	✗	✗	✗	✓	✓
Email Features					
SSL support for SMTP (outbound)	✗	✗	✗	✓	✓
Support for SMTP authentication	✗	✗	✗	✓	✓
HTML Editor Replacement for Rich Client.	✓	✓	✓	✓	✓
Time in Email Template enhanced to support 24-hour or 12-hour format.	✓	✓	✓	✓	✓
Ability to enter Email display name in IC Manager.	✓	✓	✓	✓	✓
Indication by WACD about invalid email requalification attempts.	✓	✓	✓	✓	✓

Feature	IC 7.3	IC 7.3.1	IC 7.3.2	IC 7.3.3	IC 7.3.4
Selective download of Templates based on Admin configuration	✗	✗	✓	✓	✓
Enhanced Email Migration Tool***	✗	✗	✓	✓	✓
Password encryption when login request is sent to RL Manager	✗	✗	✓	✓	✓
Support for adding multiple attachments into an email	✗	✗	✓	✓	✓
Email transcript search & sort for agents & supervisors	✗	✗	✗	✓	✓
Telephony Features					
TSA Server enhanced for Extended UUI Data Support.	✓	✓	✓	✓	✓
Adding UUID and ALIAS of TS in EDU for IVR application.	✓	✓	✓	✓	✓
HttpVOX and VOX support TS.TransferEX method.	✓	✓	✓	✓	✓
VOX Server to handle extension numbers in excess of 2^31.	✓	✓	✓	✓	✓
Monitoring IVR extension using *v assignment.	✓	✓	✓	✓	✓
SSL Enabled communication between HTTPConnector Server and Dialog Designer 5.1.	✓	✓	✓	✓	✓
Mask phone password field in IC manager	✗	✗	✗	✓	✓
Other Features					
Performance gains in SDK WebServices using DS Authentication-Only API over full DS Login.	✓	✓	✓	✓	✓
LDAP authentication support for Admin Website and RL Manager	✗	✗	✓	✓	✓
LDAP integration with Avaya Interaction Center.	✓	✓	✓	✓	✓
Restrict the retries by WACD on requesting the WAA to qualify a task when no agent is logged into IC.	✓	✓	✓	✓	✓
WebAdmin Page Cancel Task with Specified Status.	✓	✓	✓	✓	✓

Feature	IC 7.3	IC 7.3.1	IC 7.3.2	IC 7.3.3	IC 7.3.4
Workflow Server Modification for Dynamic Queue Contact Entry.	✓	✓	✓	✓	✓
Workflow Server enhanced to handle large number of Workflow channel assignments.	✓	✓	✓	✓	✓
Service Class OWT data in OA reports.	✓	✓	✓	✓	✓
Added Hyperlink button in the HTML toolbar for HTML Editor (only) in Rich Client.	✓	✓	✓	✓	✓
Reporting provision for RONA exit reason: For RONAed calls exit_reason field in the routingevent table(repository database) is populated with the value 'rona'	✗	✗	✓	✓	✓
Configuration for the Aux rona reason code.	✗	✗	✓	✓	✓
Support for chat, SCB, email form from native apps of mobile & tablet apps (IOS & Android)	✗	✗	✗	✓	✓
EWT API (with ICBA)	✗	✗	✗	✓	✓
Support for adding variable no of wrapup codes (only for AARC)	✗	✗	✗	✗	✓
Synchronization between Siebel toolbar and Hard phone.	✓	✓	✓	✓	✓
Enhanced ASIS to read IC group properties without restart.	✓	✓	✓	✓	✓
Disable 'Ready/NotReady' button if agent has not logged into any channel for IC-Siebel.	✓	✓	✓	✓	✓
VMM Service/Voice (IV) Chat	✓	✓	✓	✓	✗

*** IC 7.3.2 FP obsoletes PSN004146.

Web browsers tested in IC 7.3.4 Service Pack

Refer to **Avaya IC and OA 7.3.x Overview and Specification guide.**
Note: Collaboration features are supported in Microsoft Internet Explorer only.

IC 7.3.x interoperability with OA 7.3.x

Refer to **Avaya IC and OA 7.3.x Overview and Specification guide.**

IC 7.3.x interoperability with Communication Manager and AES

For the latest and most accurate compatibility information, go to:
http://support.avaya.com/CompatibilityMatrix/Index.aspx

Note:

Since this is a Service Pack Release, find all compatibility information in the "NOTES" Section under the IC 7.3.3 release at http://support.avaya.com/CompatibilityMatrix/Index.aspx.

Feature comparison of Avaya Agent Clients

The following table shows the feature comparisons between various Agent clients supported by IC 7.3.x:

Channel / Feature	Functionality Supported	Avaya Rich Client	Avaya Web Client	Avaya SDK Client	Avaya Siebel Native Client	Avaya Siebel Hybrid Client
Voice	Answer	✓	✓	✓	✓	✓
	Blind Transfer	✓	✓	✓	✓	✓
	Consult	✓	✓	✓	✓	✓
	Conference	✓	✓	✓	✓	✓
	Hold/Reconnect	✓	✓	✓	✓	✓
	Wrap	✓	✓	✓	✓	✓
	Transfer to Virtual Queue	✓	✓	✓	✓ *	✗
	Switch to caller	✓	✓	✓	✗	✗
	Transfer to Agent	✓	✓	✓	✓	✓
Email	Reply / Reply All	✓	✓	✓	✓	✓
	Forward	✓	✓	✓	✓	✓

Channel / Feature	Functionality Supported	Avaya Rich Client	Avaya Web Client	Avaya SDK Client	Avaya Siebel Native Client	Avaya Siebel Hybrid Client
	Defer	✓	✓	✓	✓	✓
	Use local/global resource for responses/Email Templates	✓	✓	✗	✗	✗
	Dismiss	✓	✓	✓	✗	✓
	Transfer to Agent	✓	✓	✓	✗	✓
	Transfer to Virtual Queue	✓	✓	✓	✓	✗
	HTML Editor Hyperlink toolbar button	✓	✗	✗	✗	✗
	Ability to download and use preconfigured email templates	✓	✓	✗	✗	✗
Chat	Answer	✓	✓	✓	✗	✓
	Transfer to Agent	✓	✓	✓	✗	✗
	Conference	✓	✓	✓	✗	✓
	Use local/global resource for responses	✓	✓	✗	✗	✗
	Wrap	✓	✓	✓	✗	✓
	Emoticons	✓	✓	✓	✗	✓
	Chat Typing status	✓	✓	✓	✗	✓
	Join Us	✓	✓	✓	✗	✓
	Transfer to Virtual Queue	✓	✓	✓	✗	✓
Contact History	View	✓	✓	✓	✗	✗
	Filter	✓	✓	✓	✗	✗

Channel / Feature	Functionality Supported	Avaya Rich Client	Avaya Web Client	Avaya SDK Client	Avaya Siebel Native Client	Avaya Siebel Hybrid Client
Supervisor	Monitor/Un-Monitor	✓	✓	✓	✗	✓
	Visible / Invisible	✓	✓	✓	✗	✓
Multimedia Support		✓	✓	✓	✗	✓
Selective After Call Work		✗	✗	✗	✓	✗
Variable no of Wrapup codes		✓	✗	✗	✗	✓

* This feature is supported for Avaya Siebel Native Client. However, this feature is tested only on IC Business Advocate (BA) setup on Windows.

Product updates and patches

For the latest list of all the product updates and patches, visit the Avaya Support Web site, http://support.avaya.com.
You can download the latest patches and installation instructions.

Behavioral Changes

This section lists the behavior changes introduced in IC SP/FP releases.

ACW behavior for Avaya Agent Rich Client (Introduced in IC 7.3.3 FP)

Voice channel remains in ACW when auto-in is disabled. This causes a difference in behavior between release IC 7.3.3 and the earlier one.

Avaya Agent Rich Client now acts on wrapup present event. So that after hang-up agent stays in ACW state whether Autoin is set Y or N. Consider the following scenario:

1. Login an agent with voice channel enabled.

2. Do a direct call to extension of the agent and accept it.

3. Press **ACW** from hardphone. Verify that agent hardphone shows preset ACW.

4. Hangup the call.

So after hangup, hardphone and softphone will remain in ACW state.

With the earlier release, for example, in/before 7.3.2, agent used to go in available state though ACW is pressed from Hardphone or Softphone. If agent is in manual blending mode, after hangup he can easily go available by clicking on voice channel (Softphone) or by hardphone. But if agent is in Automatic blending mode, Agent must go available by using Hardphone.

Website Logging (Introduced in IC 7.3.1 SP)

Prior to SP 7.3.1, the MTT logging and Tomcat webserver logging for website were captured in the website.log (default) log file. This behavior has changed from SP 7.3.1 onwards.

Following is the summary of changes:

1. The MTT logging continues to be captured in the `website.log`, whereas the Tomcat webserver logging for website will now be captured in the `website_debug.log` file.

2. If the website global name is other than Website, then the log file name is according to the global name, for example: `<website_context_global_name>_debug.log`. The website global name must be the same as dsObject Name as specified in `web.xml` file of website. For more information, see the IC 73 Installation and Configuration.

3. The maximum log file size specified as part of the IC Manager Website configuration applies to the `website_debug.log`. If there is no size specified, then the default `website_debug.log` size is 25 MB.

After `website_debug.log` crosses the maximum size, it rolls over into `website_debug.log.bak` and a new `website_debug.log` file is created to continue the logging.

Viewing Chat Transcript (Introduced in IC 7.3.1 SP)

View Transcript functionality in WACD Admin pages under IC **Web Self Service** > **View Transcripts** is modified from SP 7.3.1 onwards.

Following is the summary of changes:

1. New search functionality has been added. You can now type or paste a Chat ID (EDU ID) in the Call ID text box and click **Submit Query** below the search box to see the transcript for that Chat ID.

2. The existing **Select a Task-ID** drop-down continues to be present. However, the maximum number of Chat IDs fetched from the database (DB) to populate in the drop-down list is restricted.

3. Click **Submit Query** after selecting a Task ID from the **Select a Task-ID** drop-down list to display the transcript for the Chat ID selected for the first time. Thereafter, upon selection, the drop-down displays the transcript for the selected Chat ID.

4. The number of records populated in the **Select a Task-ID** drop-down is based on the following parameters that can be customized in `<AVAYA_IC73_HOME>\comp\website\admin\wtc\transcript.jsp`. This parameter is configured in `<AVAYA_IC73_HOME>\comp\website\admin\wtc\ transcript.jsp` file

   a. DefaultNTaskID: The value of this parameter defines the number of Records to be fetched from DB. This is the value used to query the DB when the **Select a Task-ID** drop-down list is populated.

      1. The default value is 200. This is can be customized to a different value between 1 and 1000.

Any value less than 1 will be treated as 200 (default).

Any value more than 1000 will be treated as 1000.

   b. LastNTaskID: Last N No. Records to be fetched from DB. This is configured in `<AVAYA_IC73_HOME>\comp\website\admin\wtc\ transcript.jsp` via DefaultNTaskID parameter.

      1. Default value is 200 which is set via DefaultNTaskID.

If LastNTaskID <=0 set LastNTaskID=DefaultNTaskID and if LastNTaskID>MaxRecord then set LastNTaskID=MaxRecord.

If NTaskID is less than or equal to 0, that is, invalid value that this value will be set to DefaultNTaskID.

If admin set LastNTaskID which is greater than 1000, which is also invalid than LastNTaskID will be set to 1000.

To perform the configuration of these parameters, refer the "Chat Transcript Configuration" section below.

Enabling Refresh AddressBook button for the ASIS server (Introduced in IC 7.3.1 SP)

When using native Siebel integration, if you add or delete an agent from IC Manager, the system does not update the ASIS server. Therefore, until you restart the ASIS server the changed agent information is unavailable. To refresh the changed agent information without the ASIS server restart, a new button **Refresh AddressBook** has been added in the ASIS server configuration.

From SP 7.3.1 onwards, when using native Siebel integration, if you add or delete an agent from IC Manager, you can click **Refresh AddressBook** in the ASIS server configuration to make the changed agent information available.

To activate the newly added **Refresh AddressBook** for the ASIS server, import the `sc.xml` file shipped with SP 7.3.1 or later by following the steps mentioned in "Merging and importing the sc.xml" section below in this document.

Changes to ICM Server and CIRS Log files
(Introduced in IC 7.3.1 SP)

The ICM server log file name, `icmlog.txt`, is now `icmserver.log` in SP 7.3.1. The name of the backup log file created upon rollover of ICM log is changed to `icmserver.bak`. The CIRS log file, `cirslog.txt` is now `cirslog.log` in SP 7.3.1. The name of the backup log file created upon rollover of CIRS log has been changed to `cirslog.bak`.

The name of the property **Maximum Property Management Log Size (KB)** is now **Maximum ICM Log size (KB)** in SP 7.3.1.

The **Maximum ICM Log size (KB)** parameter defines the maximum size of `<globalicmname>_website.log` file. The **Maximum ICM Log size (KB)** parameter also defines maximum size of the `icmserver.log` if the value is greater than 10240 KB.

The minimum size of `icmserver.log` is 10240 KB. If the value of **Maximum ICM Log size (KB)** parameter is set to lower than 10240 KB in IC Manager, the ICM server treats the maximum size of `icmserver.log` as 10240 KB.

To perform the configuration of these parameters, refer "Configuration related to ICM Server and CIRS Log files" section below.

ChannelWeightFactor for Business Advocate
(Introduced in IC 7.3.1 SP)

The Least Occupied Agent (LOA) or Most Idle Agent (MIA) algorithms of IC Business Advocate are enhanced to use additional attribute of ChannelWeightFactor. ChannelWeightFactor has been part of IC from IC 7.1 onwards. ChannelWeightFactor lets you assign a weight factor for each channel, allowing for additional channel priority selection.

As documented in the Administration Guide, you can configure the weight factor for every channel by setting the ResourceManager Server configuration attributes:

- ChannelWeightFactorVoice – for voice calls.

- ChannelWeightFactorChat – for chat contacts.

- ChannelWeightFactorEmail – for email contacts.

Each of these attributes can be set to an integer. When the attribute is not configured, the default value is 1.

Description of the ChannelWeightFactor

Resource Manager multiplies the ChannelWeightFactor for each channel by the number of contacts that are currently serviced by the agent for that channel. The resulting value is called the Weighted Contact Value of the agent. The Weighted Contact Value is calculated for every channel of every agent.

RM selects the next available agent that has the lowest value of Weighted Contact Value. For example:

Two agents are configured to handle maximum two contacts at a time – with two voice or two chats or one voice and one chat at the same time. Both the agents have the voice and chat channels enabled.

When ChannelWeightFactor is not specified, the behavior is as follows:

1. Agent1 and Agent2 are available.

2. A new call arrives and is matched to Agent1.

3. A new chat arrives and is matched to Agent2.

4. Another new chat arrives and is matched to Agent1.

RM using the LOA and MIA algorithms can select agent1 to deliver the second chat.

There might be a requirement to send the second chat to Agent2 although this agent might not be the selected agent using LOA or MIA algorithm. The reason for this selection is that preference is given to voice channel over chat channel. Therefore, one agent handling two chats simultaneously might be preferred over one agent handling one voice and one chat at the same time.

This can be achieved by setting the configuration attributes:

- ChannelWeightFactorVoice = 2

- ChannelWeightFactorChat = 1

With this configuration, the behavior changes as follows:

1. Agent1 and Agent2 are available.

2. A new call arrives and is matched to Agent1.

    a. Weighted Contact Value = ChannelWeightFactorVoice * Number of voice calls currently serviced by the agent.

    b. Therefore, Weighted Contact Value for Agent1 = 2 * 1 = 2.

3. A new chat arrives and matches to Agent2.

    a. Weighted Contact Value = ChannelWeightFactorChat * Number of chat contacts currently serviced by the agent.

    b. Therefore, Weighted Contact Value for Agent2 = 1 * 1 = 1.

4. A new chat arrives. This chat matches with Agent1 or Agent2 as both are enabled for the chat channel.

However, Weighted Contact Value for Agent2 is lesser than Weighted Contact Value for Agent1.

Hence, the chat is delivered to Agent2.

Logging for Business Advocate Agent Watcher (Introduced in IC 7.3.1 SP)

Logging support is added for Business Advocate Agent Watcher from SP 7.3.1 onwards. Agent Watcher creates a log file in `<AVAYA_IC73_HOME>\logs` folder with the name `AgentWatcher.log`.

The `AdvocateSetup.log` file is used to capture the log messages from the Business Advocate Config Tool. The following configuration parameter is applicable to the `AdvocateSetup.log` file as well.

To configure the log file size, add the following section in the mosaix.ini file located in the nethome folder:

```
[Debug]
LogFileSize=10
```

If you do not configure this parameter, the default log file size is 10 MB. One backup file is created when the log file rolls over.

UTF-8 Encoding for outgoing emails from WebAgent (Introduced in IC 7.3.1 SP)

The current behavior is an agent can select a character set of an outgoing email. If the agent does not select any character set exclusively, the system sets a default character set. The default character set that is usually the top character set in the list, gets selected which can cause issues with email rendering at the end customer.

To address such issues, the WebAgent behavior is changed in SP 7.3.1 to check if an email body can be encoded using UTF-8 encoding irrespective of the character set selected by the agent.

An email is sent with UTF-8 encoding when the following conditions are met:

1. The email body of the outgoing email cannot be completely encoded in the selected character set either explicitly selected by the agent or by default selection.

AND

2. Either one or both of the following conditions:

   ▪ Attribute `email.charsetdetection.coverttoutf8` is set to true.

   ▪ If an email body can be completely encoded using UTF-8.

In all other cases, an email is sent in the selected character set.

Note: The default value of the parameter `email.charsetdetection.coverttoutf8` is true. It can be set to false using the steps below:

1. On the AARC computer, open `<AVAYA_IC73_HOME>\Webagent\Application.properties` file using a text editor.

2. Search if the `email.charsetdetection.coverttoutf8` parameter is present or add if it is not present.

3. Change or add the following: `Email.charsetdetection.converttoutf8 = false`

Note: If the parameter email.charsetdetection.coverttoutf8 is not present in Application.properties file, the behavior is same as when the value is 'true'.

Behavior change for Push URL and Co-browse (Introduced in IC 7.3.1 SP)

The collaborative form filling/Co-browse and Push URL will work with the website supporting IFrame only. This has observed with following web browsers:

- Internet Explorer 10 (32-bit only) and onward
- Mozilla Firefox
- Chrome

On pushing URL, sites handling "Click Jacking Security" will override the chat window.

Enhancements in IC 7.3.4 Service Pack

Java Upgrade

Java runtime has been upgraded from JRE 6u45 (32-bit only) to JRE 8u40 (32-bit only) on Windows platform and JRE 6u45 (32-bit only) to JRE 7 (32-bit only) on Solaris Platform.

Note: As per the **JRE Expiration** policy of Oracle, the current version of Java expires whenever a new release with security vulnerability fixes becomes available. For systems unable to reach the Oracle Servers, a secondary mechanism (hard-coded expiration date) expires the JRE. After either condition is met (new release becoming available or expiration date reached), Java will provide additional warnings and reminders to users to update to the newer version.

For more information see "23.1.2 JRE Expiration Date" section on the Oracle Website: http://docs.oracle.com/javase/8/docs/technotes/guides/deploy/client-security.html

You will see following error when JRE minimum requirement (of having JRE 8u40 (32 Bit)) does not meet on Agent machine. Please refer "Prerequisite" section for more information.
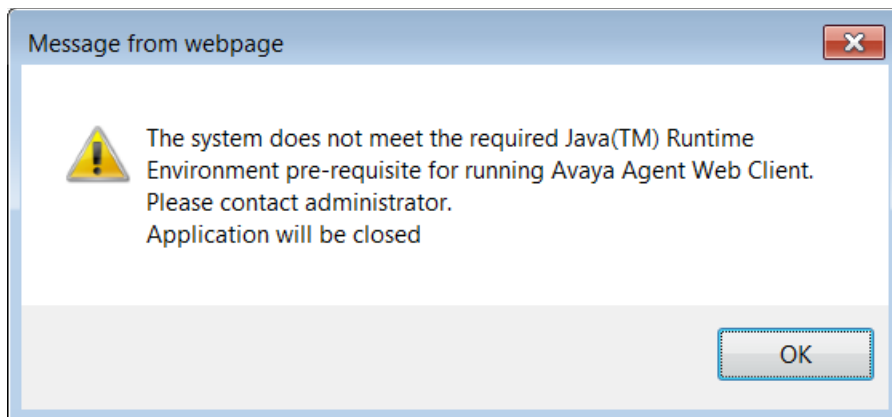
Support for changing the default selections of Tab focus and Site drop down in UAD

In AARC UAD the site selected in the drop down and the tab which has the focus, by default can now be customized. To achieve this the UAD now exposes two APIs, SetSite and SetCustomTab which can be invoked from the AARC scripts. Using these APIs the default site and the tab focus can also be changed for different operations done by the agent. For instance, clicking on the initiate button for a voice contact can have a different set of selection for site & tab focus as opposed to clicking the conference button. Please refer the Avaya Agent Integration guide for details on how to use these APIs.

Variable number of Wrapup code types

From 7.3.4 SP, you can add up to seven more wrapup code types in addition to existing "Reason" and "Outcome" code types.

For more information see "Configuration" section to configure this feature.

Added a support for dot and hyphen for agent usernames

In IC 7.3.4, you can create Agent Id having dot and hyphen characters.

For example - john.smith_en

Note:

- Existing rule allows Agent ID to begin with alphabet only. That will not change.

- Existing rule of allowing Agent ID to begin with alphabet will remain same.

Enhancements in IC 7.3.3 Feature Pack

Email Filter to support regular expressions.

The email management allows the administrator to define regular expressions for filtering emails that can or cannot send messages to Avaya IC email accounts or queues. The Email Management checks an incoming email address for the presence of a substring that matches the regular expression pattern. You can filter a complete email address, such as **friend@public.com**, or a substring within the email address, such as **spam.** The pattern matching by default is case sensitive. You can define a regular expression to configure case insensitive pattern matching.

Please refer 'Creating email filters in IC 7.3.3' section in the **Administration Guide** for details on how to create email filters.

Email Filter tool for sampling filter regex enhancement

The Email Filter tool has been provided in the Design and Admin package for the administrator to test regular expression strings provided as email filters against the expected incoming email addresses. The tool provides the administrator the feasibility of testing whether or not an email address will be accepted/rejected (depending upon the type of filter selected) by the Poller server based on the regular expression provided.

Please refer '**Email tool for testing the regex filter**' section in the Administration **Guide** for details on how to use this tool.

Deprecate SSLv3 and below for SSL/TLS communication

1. OpenSSL library version is upgraded from 0.9.8d to 0.9.8zc.

2. IC SSL/TLS enabled severs, for example, Directory Server (DS), HTTPConnector Server are modified from 7.3.3 FP onwards to accept only TLSv1.0 during TLS handshake

3. IC SSL/TLS clients, for example, AARC, AAWC now uses TLSv1.0 during TLS handshake.

4. A client from an older version of IC cannot communicate with an upgraded 7.3.3 DS for 'Login' or 'Authenticate' requests. However to enable such communication during upgrade scenarios, the flag 'allow_sslv3' must be turned on in DS. To turn on the flag perform the following:

    a.   Login to IC Manager with Admin privileges.
    b.   Edit the DS.

    c.   Go to the **Configuration** tab.

    d.   Click the **New** to open the 'CTI Type Editor'.

    e.   Provide the values for this new couple as:

         – Name: allow_sslv3

         – Value: 1

    f.   Click **OK**.

    g.   Click **OK** of DS Editor.

    h.   Restart the DS in IC Manager.

    i.   Repeat steps a to h for all DSs configured in the IC system.

Note: The property must be removed when the clients are upgraded to IC 7.3.3.

Idle Timeout Tenant Properties Support

`<AVAYA_IC73_HOME>\comp\csportal\WEB-INF\Localized.properties`

1. See Admin guide for configuring chat idle timeout properties.

2. Add the following properties in the already mentioned file:

    a.   `chat.htmlclient.customer.inactivitytimer.enabled.`

    b.   `chat.htmlclient.customer.inactivity.totaltime.`

    c.   `chat.htmlclient.customer.inactivity.countdowntime.`

Support for MS SQL 2012, MS SQL 2014 and Oracle12C database

To support MS SQL 2012, MS SQL 2014 and Oracle 12C database, the new options for ODBC drivers are provided in the following:

- Config tool.

- ICManager.

- Database Designer.

IC 7.3.3 supports the following:

- Providing only on Windows operating system.

- Providing support Oracle 12C, but without pluggable database container.

You can provide the ODBC driver value on the **Dataserver configuration** tab in IC Manager and in DB Designer. The value that you provide on the **Dataserver configuration** tab overrides the value that you provide in DB Designer.

Config tool – SQL native client support

When you configure the website in IC, the Config tool creates DSN for PDM to communicate with the database.
Earlier, you create these DSNs with the default ODBC driver, SQL Server, which is shipped with Windows operating system. Now, Microsoft has deprecated the driver and cannot support it in future versions of Microsoft operating system.
To support the new ODBC drivers, new options are provided in the Config tool. The tool is to support the Native client, which is available with SQL 2008, SQL 2012 and SQL 2014. You must select the appropriate ODBC driver for PDM.
In the Config tool you can view the new field, **SQL Driver (Windows Only)** on the **Web** tab. This field lists the following options:

- SQL Server (Installed with Windows OS).

Note: This option will be removed in future builds.
- SQL Server Native Client 10.0 (Installed with SQL Server2008).

- SQL Server Native Client 11.0 (Installed with SQL Server2012).

- SQL Server Native Client 11.0 (Installed with SQL Server2014).

Note: The **SQL Driver (Windows Only)** field lists only the drivers that you installed on the system.
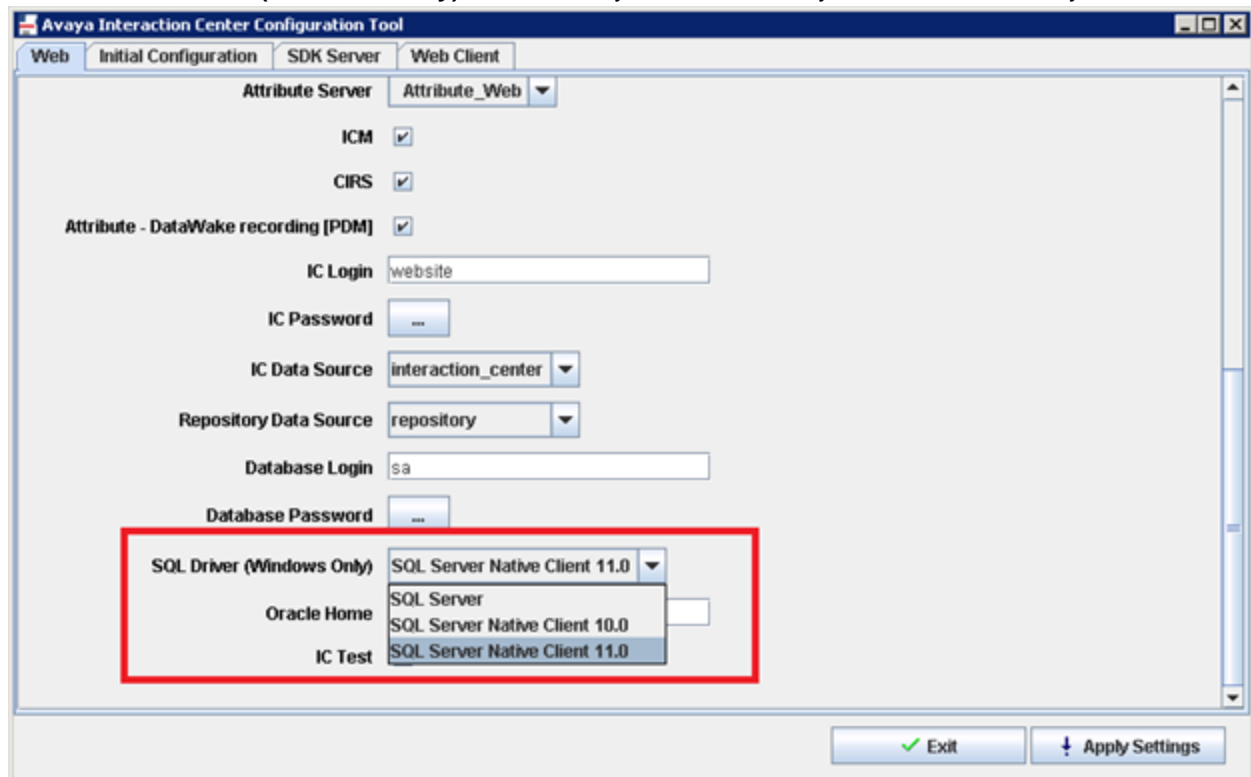
Note: You can also access the registry to verify the installed ODBC drivers.
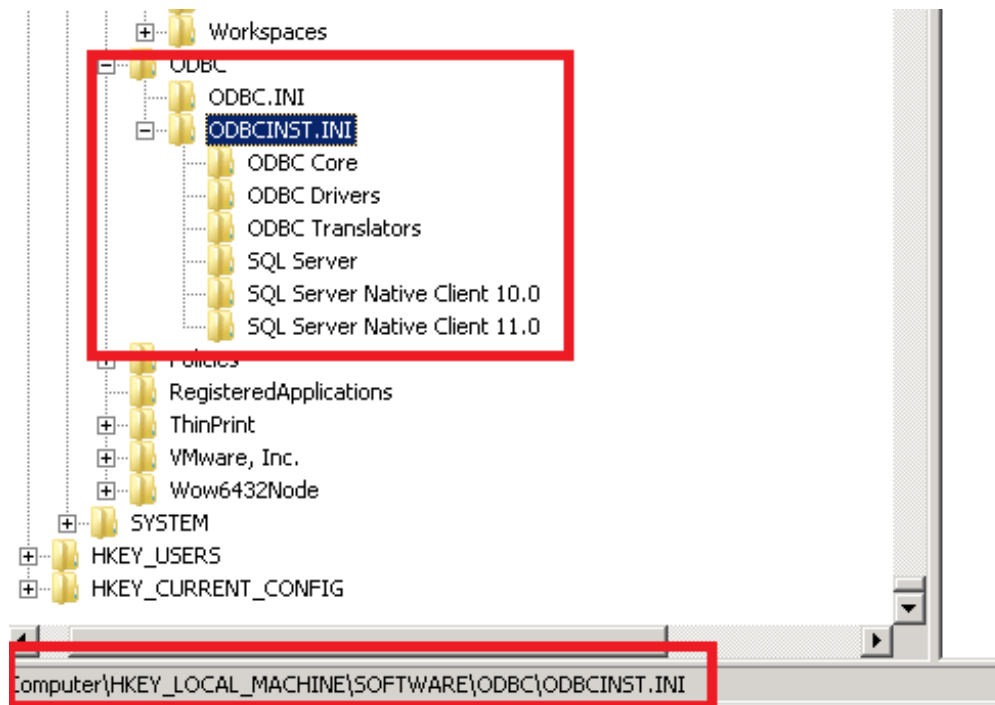
Database Designer – SQL native client support

To communicate with the SQL database, the DataServer uses connection string, which is an input parameter for the ODBC driver. This connection string contains the ODBC driver name.

Earlier in IC, this connection string was using the default ODBC driver named SQL Server, which is installed by Windows operating system. Now, Microsoft has deprecated the driver and cannot support it in future versions of Microsoft operating system.

To support the new ODBC drivers, a new parameter is added in Database Designer (DB Designer) to support the Native client, which is available with SQL 2008 and SQL 2012. You must manually enter the appropriate ODBC driver before configuring the ccq and repository databases.

In DB Designer, you can view the new parameter ODBC Driver Name on the Properties tab. For this parameter, you must manually enter the appropriate value from the following options:

- SQL Server (Installed with Windows OS).

Note: This option will be removed in future builds.

- SQL Server Native Client 10.0 (Installed with SQL Server2008).

- SQL Server Native Client 11.0 (Installed with SQL Server2012 and SQL Server2014).

In DB Designer, you can access the ODBC Driver Name parameter as follows:

1. Open the DB Designer application.

2. In the left pane, select **Physical DB Connections** > **ccqDBConnection**.

3. On the **Properties** tab, expand the Options node in the Database Connection Parameters area.

4. For the ODBC Driver Name parameter, specify the appropriate value.

Note: For the ODBC Driver Name parameter, you must specify the driver name that you installed on the system.
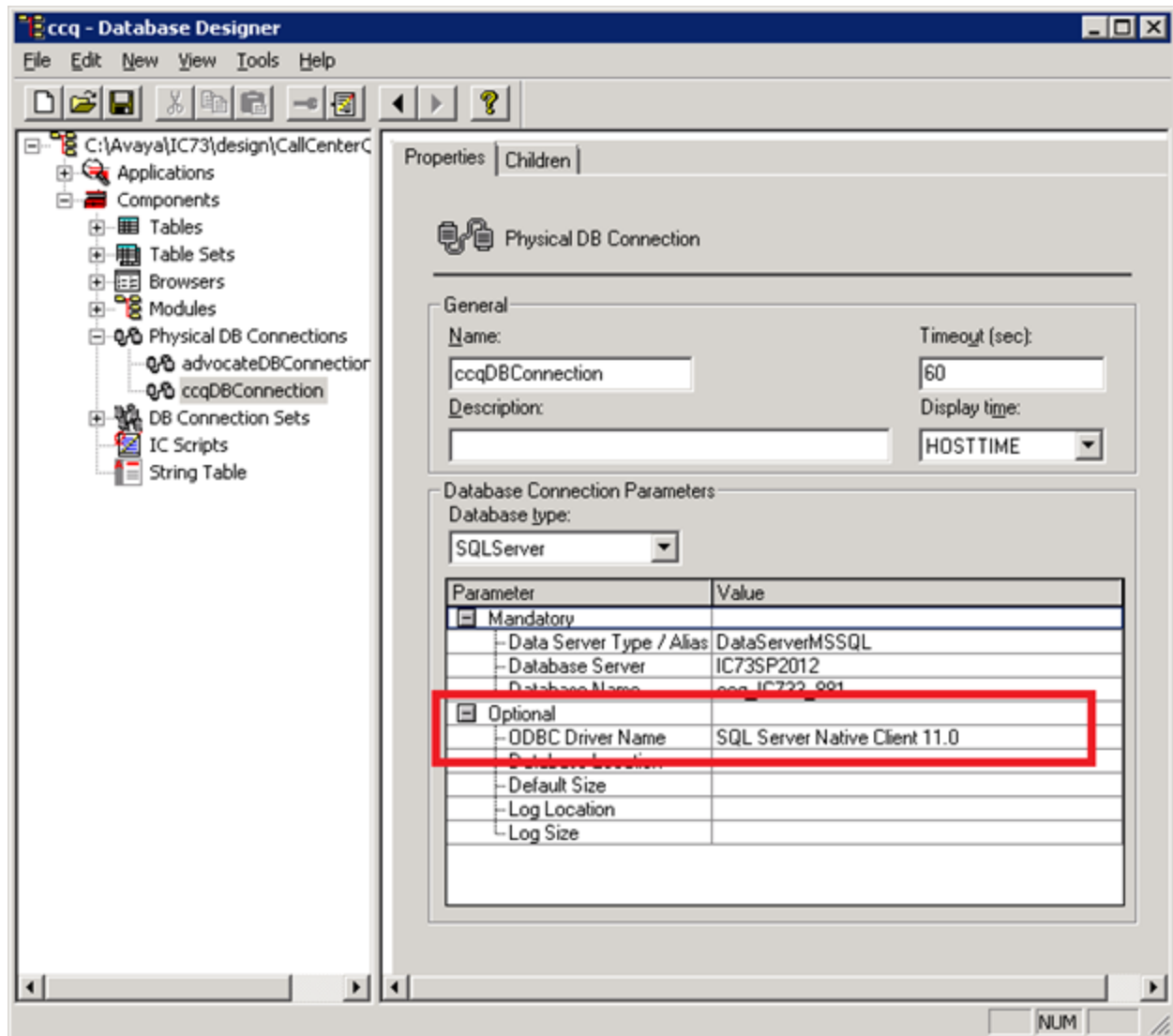
Oracle 12C database

In the Avaya IC Configuration Tool a new Oracle version is added. The **Oracle Version** field displays Oracle 12.
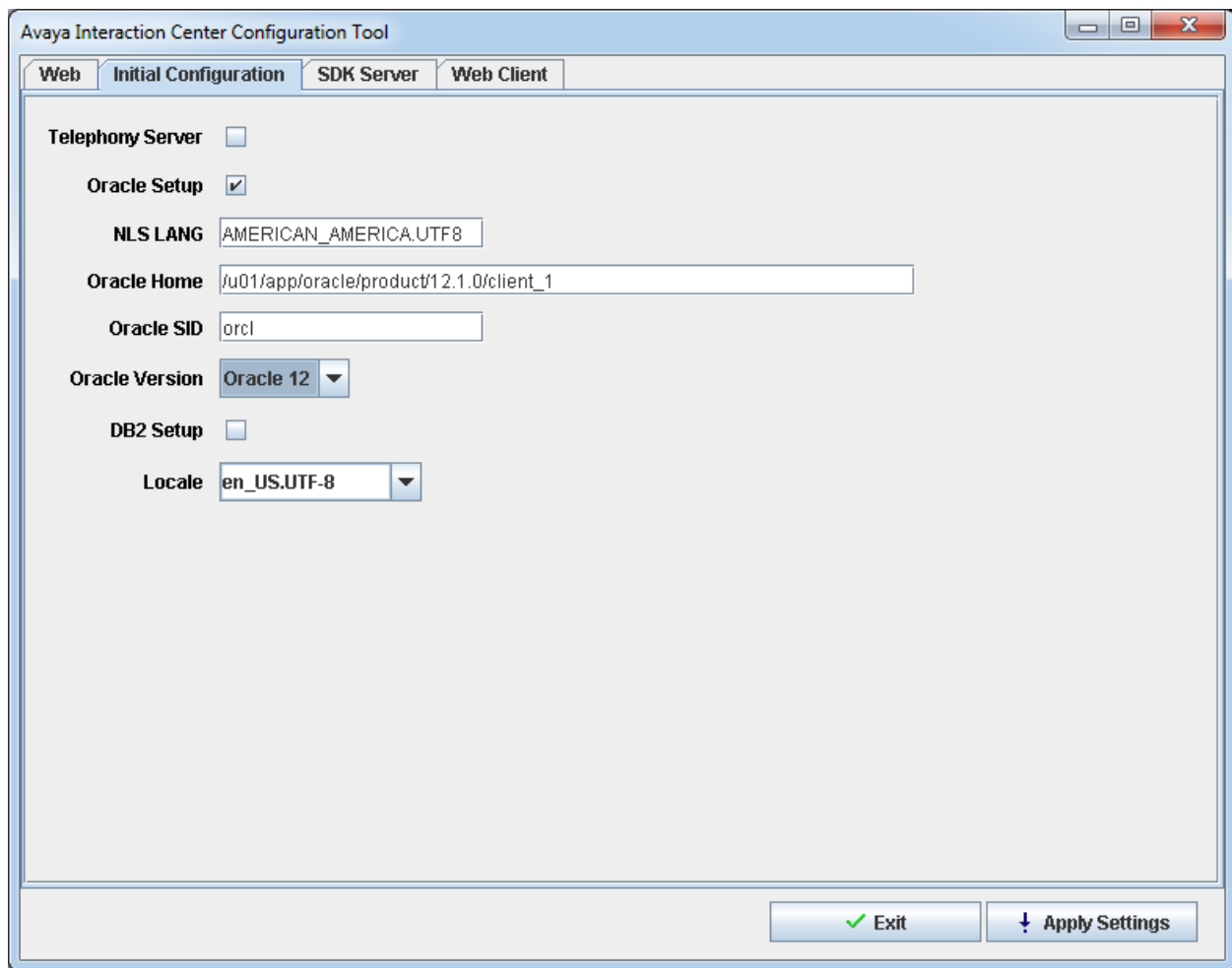
To configure database with a fresh Installation of Oracle 12 perform the following:

1. Installation steps for IC Server Machine:

   a. Install Oracle12C client on IC machine on Windows/Solaris platform.

   b. Launch Avaya IC Configuration Tool.

   c. In the **Oracle Version** field click Oracle 12.

   d. Provide client path.

   e. Click **Apply Settings**.

2. Database Configuration steps for Design Admin Machine:

   a. Launch DB Designer.

   b. Provide all required details as shown in the following screenshot for ccq and repository.

   c. Configure database.

Note: The following fields are mandatory while configuring Oracle database with 12C in DB Designer.

ccq.adl - Database Designer

File Edit New View Tools Help

C:\Avaya\IC73\design\CallCenterQ\ccq.a
  Applications
  Components
    Tables
    Table Sets
    Browsers
    Modules
    Physical DB Connections
      advocateDBConnection
      ccqDBConnection
    DB Connection Sets
    IC Scripts
    String Table

Properties | Children

Physical DB Connection

General
  Name: Timeout (sec):
  ccqDBConnection   60
  Description: Display time:
                                           HOSTTIME

Database Connection Parameters
  Database type:
  Oracle

Parameter	Value
Mandatory	
Data Server Type / Alias	DataServerOracle
TNS Name	ORCL
Database Name	ccq_167_new
Client Library Home Directory	/u01/app/oracle/product/12.1.0/client_1
Optional	
Default Tablespace Name	USERS
Default Tablespace Size	UNLIMITED
Temp Tablespace Name	TEMP

Ready   NUM

These fields are present under heading Optional. Now a message box displays to enter these values explicitly.

- Default Tablespace Name (Default value: USERS).

- Default Tablespace Size (Default value: UNLIMITED).

- Temp Tablespace Name (Default value:TEMP).

ICManager – SQL native client support in DataServerMSSQL

To communicate with the SQL database, the DataServer uses connection string, which is an input parameter for the ODBC driver. This connection string contains the ODBC driver name.

Earlier in IC, this connection string was using the default ODBC driver named SQL Server, which is installed by Windows operating system. Now, Microsoft has deprecated the driver and cannot support it in future versions of Microsoft operating system.

To support the new ODBC drivers, a new field is added in ICManager to support the Native client, which is available with SQL 2008, SQL 2012 and SQL 2014. You must appropriately select the ODBC

In the ICManager, you can view the new field, **SQL Driver (Windows Only)** on the **DataServer** tab in the DataServer configuration.

This field lists the following options:

- SQL Server (Installed with Windows OS).

Note: This option will be removed in future builds.

- SQL Server Native Client 10.0 (Installed with SQL Server2008).

- SQL Server Native Client 11.0 (Installed with SQL Server2012 and SQL Server2014).

Note: The **SQL Driver (Windows Only)** field lists only the drivers that you installed on the system.
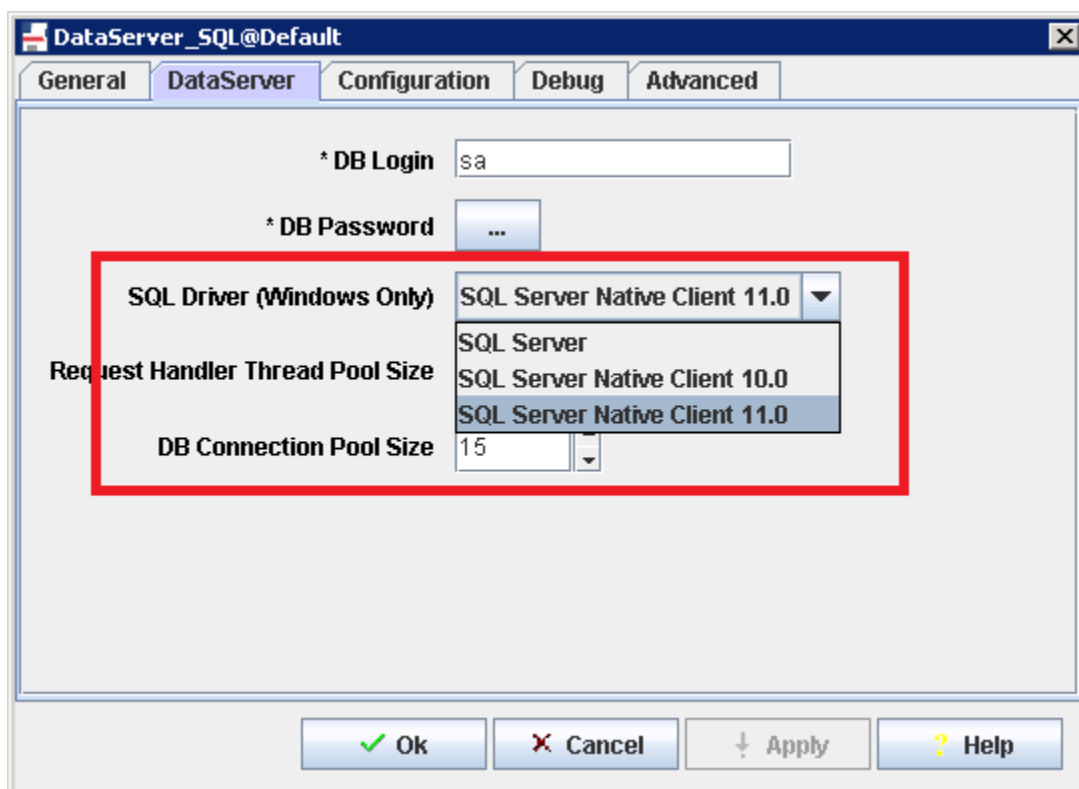
Config Accelerator - SQL native client support

To communicate with the SQL database, the DataServer uses connection string, which is an input parameter for the ODBC driver. This connection string contains the ODBC driver name.

Earlier in IC, this connection string was using the default ODBC driver named SQL Server, which is installed by Windows operating system. Now, Microsoft has deprecated the driver and cannot support it in future versions of Microsoft operating system.

To support the new ODBC drivers, a new parameter is added in Config Accelerator to support the Native client, which is available with SQL 2008, SQL 2012 and SQL 2014. You must manually enter the appropriate ODBC driver before configuring the ccq and repository databases.

In Config Accelerator, you can view the new parameter ODBC Driver Name on the Properties tab. For this parameter, you must manually enter the appropriate value from the following options:

- SQL Server (Installed with Windows OS).

Note: This option will be removed in future builds.

- SQL Server Native Client 10.0 (Installed with SQL Server2008).

- SQL Server Native Client 11.0 (Installed with SQL Server2012 and SQL Server2014).
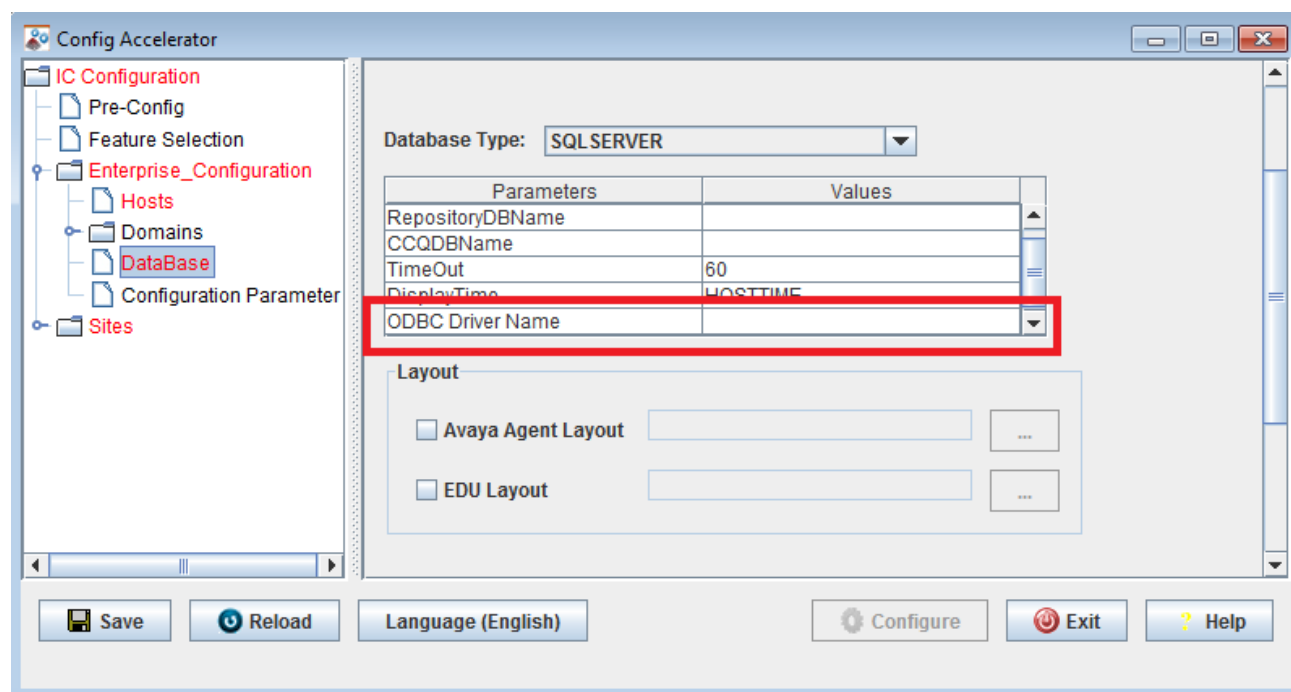
Oracle 12C database

While configuring the Oracle database with Oracle 12C in Config Accelerator, the following fields are mandatory:

- Default Tablespace Name(*Oracle12C)

- Default Tablespace Size(*Oracle12C)

- Temp Tablespace Name(*Oracle12C)
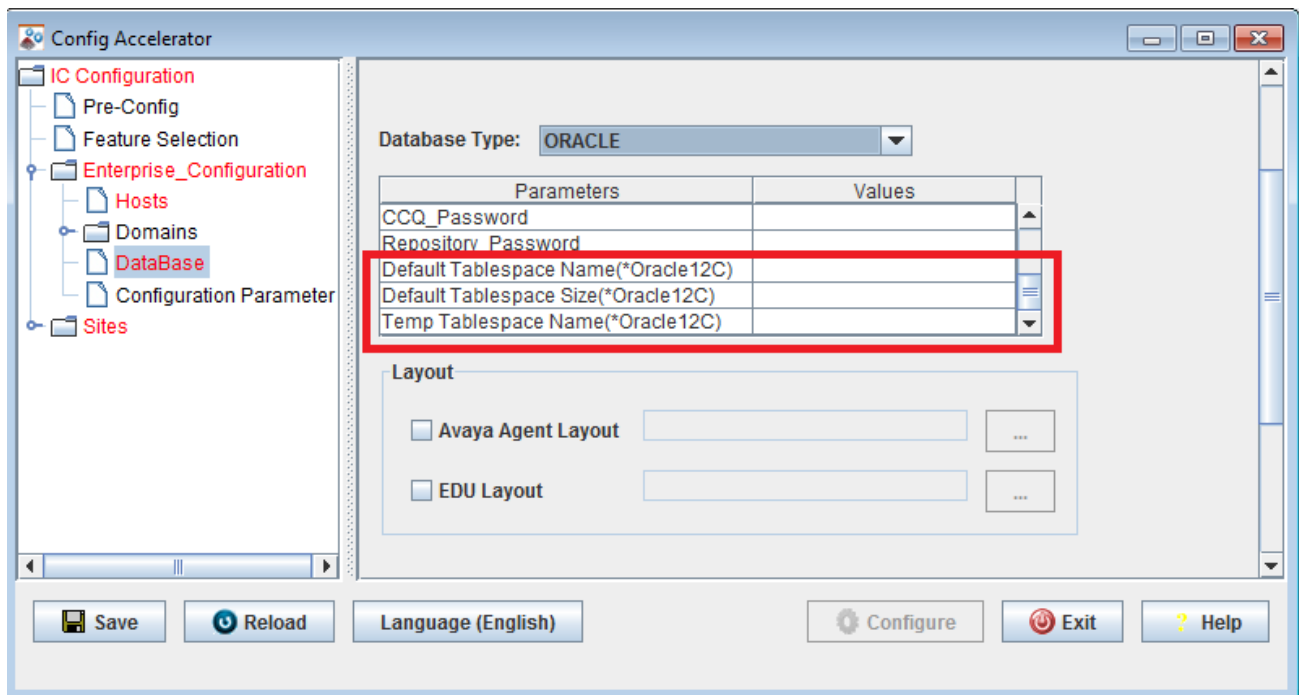
Configuring IC with new database

Fresh Installation

1. Install SQL 2012 or SQL 2014 client on the system where you must configure DataServer.

2. Install 7.3 RTM and install 7.3.3 FP.

3. Run the Avaya IC Configuration Tool.

4. While creating Dataserver SQL, on the DataServer tab in the **SQL Driver (Windows Only)** field click on the SQL Server you want to run.
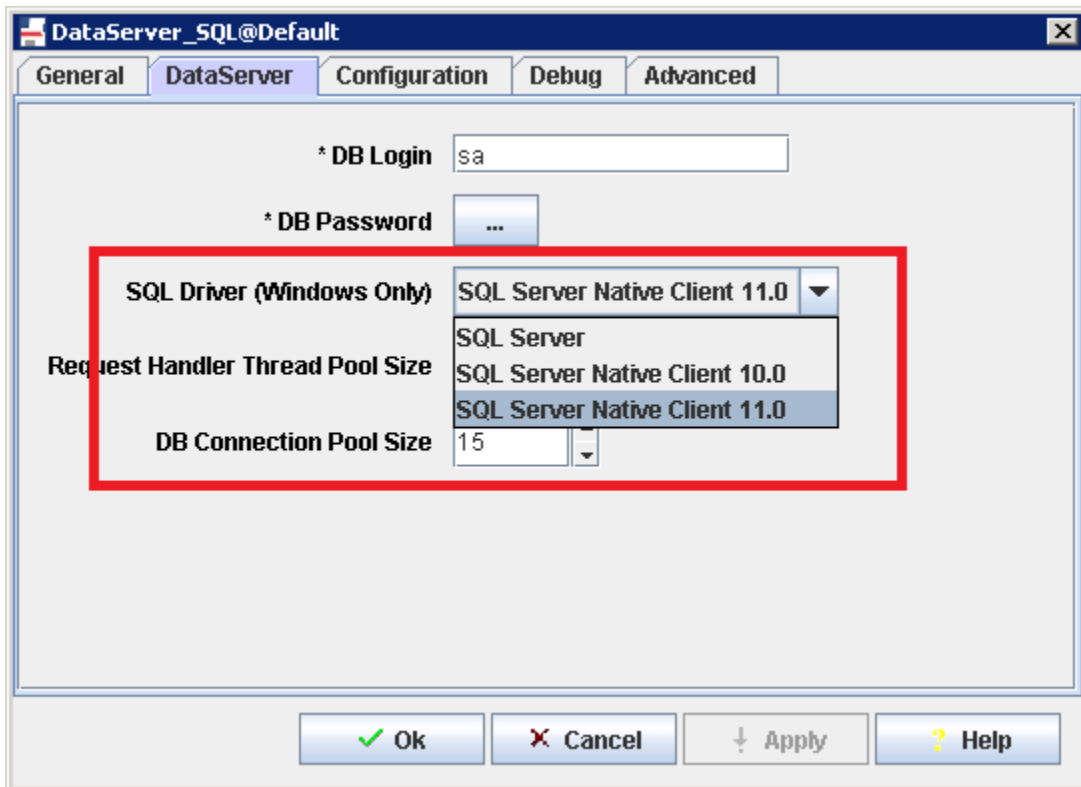
5. Run DB Designer.

6. Add required details for SQL server.

7. Add entry for ODBC driver name.
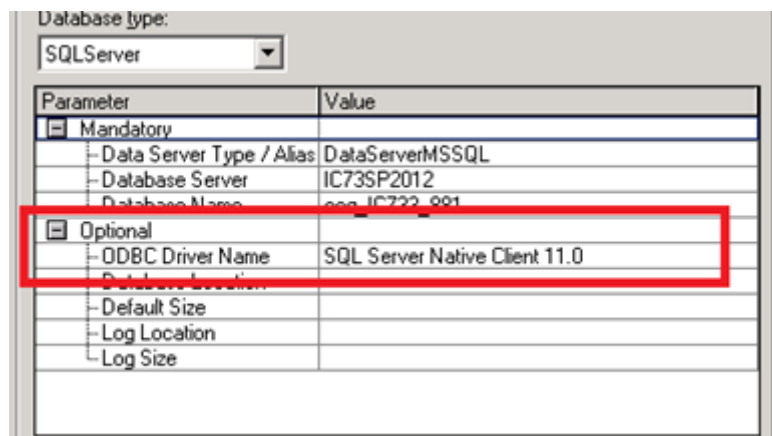
8. Configure database for both ccq and repository.

To verify which ODBC driver name is used by DataServer, verify in the logs for dbHome:

```
!F_OPEN_DIRECT_CONNECTION: Swap_flag=0,dbName=ccq_IC733_881,dbHome=SQL Server Native
Client 11.0,dbSvr=IC73SP2012
```

Note: If you enter value for ODBC driver in DB Designer and in the configuration of DataServer, DataServer overrides value provided by DB Designer with the value of the configuration.

---

9. In IC Manager, import sc.xml from `AVAYA_IC73_HOME\etc` folder.

10. When configuring a website, in the **SQL Driver (Windows Only)** field click on the SQL Server to create DSN for PDM.

11. Apply settings in Avaya IC Configuration Tool.

12. Verify that DSNs are created with the correct ODBC drivers.
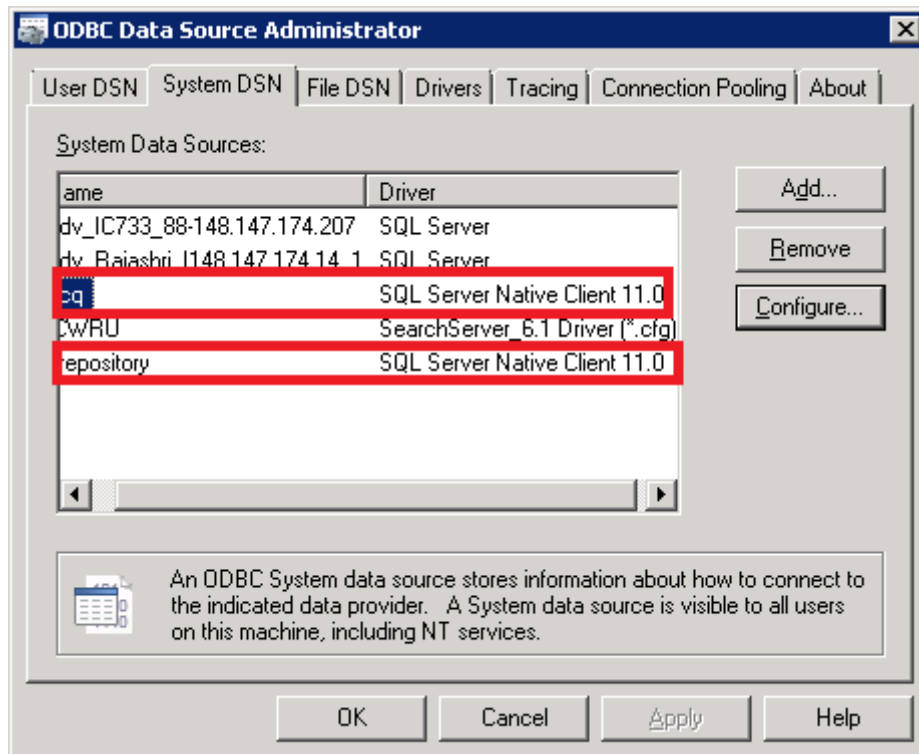
Migration of database from SQL 2005 or SQL 2008

Assumption: IC 7.3.x is installed and configured with SQL 2005 or SQL 2008 DB

1. Stop IC server and all services.

2. Take backup DBs for ccq and repository from SQL 2005 or SQL 2008.

3. Restore the backups taken in SQL 2012.

Comments on this document? infodev@avaya.com

4. Install 7.3.3 FP.

5. Start ORB server.

6. Start IC Manager.

7. Set the value for **SQL Driver (Windows Only)** in DataServer.

8. Start DataSever.

9. Open DB Designer.

10. Add entry for ODBC driver name.

11. Update DataBase Server name (SQL 2012 server or SQL 2014 server).

12. Reconfigure DB for ccq and repository with new database.

Upgrade SQL 2005 or SQL 2008 to SQL 2012 or SQL 2014.

Assumption: IC 7.3.x is installed and configured with SQL 2005 or SQL 2008 DB

1. Stop IC server and all services.

2. Back up the ccq and repository databases from SQL 2005 or SQL 2008.

3. Restore the backups in SQL 2012 or SQL 2014.

4. Apply 7.3.3 patch.

5. Start ORB server.

6. Start IC Manager.

7. Set the value for **SQL Driver (Windows Only)** in DataServer.

8. Start DataSever.

9. Open DB Designer.

10. Add entry for ODBC driver name.

11. Update DataBase Server name (SQL 2012 server or SQL 2014 server).

12. Reconfigure DB for ccq and repository with new database.

SMTP Authentication with TLS and secure Authentication

In Avaya IC, when sending an outbound email, the ICEmail server uses the options that you configure for an email account in IC Manager on the **Outgoing Email Server** tab.

Currently IC Manager has the provision to provide Outgoing Email Server (SMTP) server information with the default port used as "25".

To support the SMTP Authentication with TLS and Secure Authentication for an outgoing email communication, new fields are added in IC Manager on the **Outgoing Email Server** tab.

The new fields are the following:

- Use TLS:
    - None
    - TLS
    - STARTTLS
- Use SMTP Authentication:
    - Logon account
    - Password
    - Confirm
    - Use Secure Authentication:
        - Authentication Type:
            - o NTLM
            - o CRAMMD5
            - o LOGIN

New fields added for supporting the SMTP & SSL support:

In IC Manager, if the administrator wants to enable the secure communication and SMTP Authentication for a configured email account, the administrator must select the **Use TLS** and **Use Secure Authentication** fields.

Selecting the value in the **Use TLS** drop-down list as "TLS" changes the default port 25 to 465 as the secure communication port. Also, to have the SMTP Authentication, the administrator must provide a valid email account configured on the exchange with account password, so that the ICEmail server can authenticate the account when sending an email.

IC Manager also facilitates the administrator to select the type of encryption needed to use for the password while authenticating the email account. However, the administrator must ensure that the selected Authentication type is supported by the exchange.

By default, IC Manager uses the "PLAIN" Authentication type.

Administrator has to install the client certificate in the Avaya core server system, the ICEmail server machine, under the `\etc` folder as a keystore for the ICEmail server. The name of the certificate used is `<smtp server name>.pem`.

When sending an outbound email, ICEmail reads the configured values for the email account from the database table `qem_mailaccount`. ICEmail checks if the SMTP for the account is using the TLS, SMTP authentication and type of authentication or not. The following columns read these values:

Column Name	The Outgoing Email Server tab in IC Manager
enablesmtptls	Use TLS
enablesmtpauth	Use SMTP Authentication
smtpmailbox	Logon account
smtppassword	Password

Column Name	The Outgoing Email Server tab in IC Manager
smtpsecurepassword	Use Secure Authentication
smtpauthtype	Authentication Type

SMTP Authentication and TLS configuration for the chat transcript email

As a part of the secure communication, the outbound email that IC Manager sends to provide the customer the chat transcript is sent using the SMTP authentication or using the TLS, depending on the account configuration in the IC Manager.

When a customer escalates a chat, the website component fetches the SMTP host name from the configured emails accounts. This SMTP host information is further passed to the ICM server so that it can be used to send the chat transcripts to the email account of the customer. The website picks the first configured email account in the IC Manager and sends the SMTP host information for this account to the IC Manager Server. If no account is configured, IC Manager Server uses the SMTP host configured on the configuration tab in the ICM tree node.

The new design requires that an email account must be present in the IC Manager. The new design must be present so that the SMTP host and other security related configuration are provided to the ICM by the website. The configuration can be provided for sending the chat transcript email at the email address of the customer. The configuration for the email account becomes mandatory because the SMTP host configuration for the IC Manager in the configuration tab of the IC Manager does not exist.

If no email channel is configured for the AIC system, still the administrator has to configure at least one email account in the IC Manager. This configuration is done so that IC Manager can use the SMTP host and other information to send the chat transcript email. Also, the administrator has to configure a dummy poller cluster which cannot poll any email account. To use the TLS setting, the administrator must put the client certificate from exchange server in the keystore of the IC Manager Server system. This client certificate is put in the java keystore as the IC Manager Server is in java.

SMTP Authentication and TLS configuration for the email send from the website to the IC system

The Avaya IC website facilitates the customer to send an email into the AIC system from the public website. The AIC website uses the SMTP host for the first email account configured for the tenant of website

Currently the website does not have any provision to provide the SMTP authentication and TLS for the email communication into the AIC system.

The new design uses the first configured email account. If the email account is configured for the SMTP authentication and TLS, the website sends the email into the AIC system accordingly.

Note: To use the TLS setting, the administrator must add the client certificate from exchange server in the Keystore of the Website server system. This client certificate is put in the java keystore as the Website server is in java.

Chat time Stamp Feature

When an agent is handling a chat contact no timestamp is shown with the chat messages. However, the old website, after enabling the timestamp property from the admin site, and csportal does show the timestamp for each chat message at customer end. As a part of this enhancement the chat messages show at the agent end also contains the time stamp when enabled on the IC Manager Server configuration.

Design:

The chat messages are broadcast by the IC Manager server. So when a chat message is send by the agent or customer IC Manager Server adds a UTC time as a new parameter with the Transcript object. Depending on the time zone agent application converts the UTC time to local time zone.

Note:

1. The time stamp is not shown with the system phrases such as caller type, transfer/Conference phrases, supervisor entering/leaving the chat room phrases.

2. The time stamp shown at the customer end website/csportal is actually using the ICM time and timezone to sync/adjust chat transcript time with his system local time zone.

To configure the enabling of the chat time stamp for the agent perform the following:

1. On the IC Design and Admin machine import the new sc.xml file from the IC Manager.

2. After successful import re-launch IC Manager

3. Go to the IC Manager configuration tab.

4. A new check box, **Enable Agent Timestamps**, is present to enable the time stamp.

5. Select **Enable Agent Timestamps**.

6. Restart the IC Manager service.

Note: OOTB the **Enable Agent Timestamps** is disabled. The administrator has to explicitly enable this to use the agent side time stamp feature.
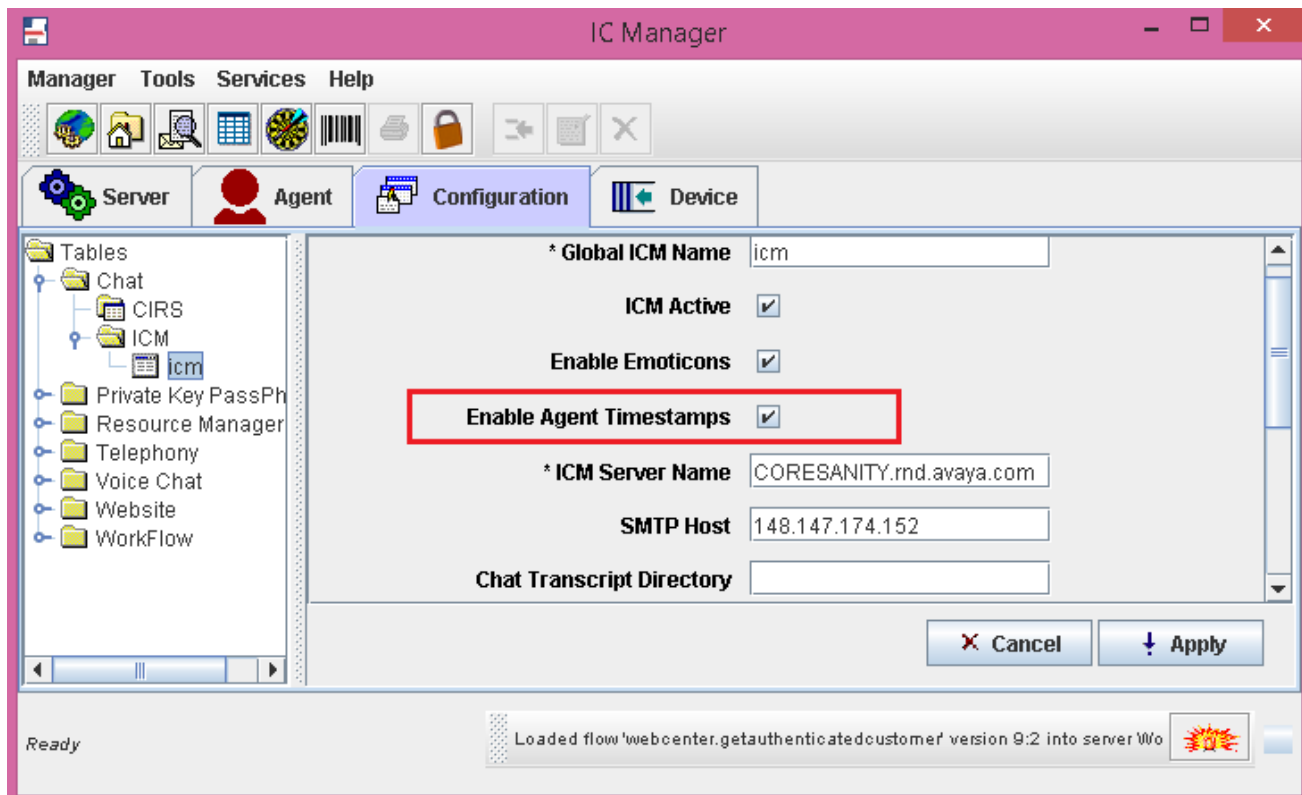
ASG Plugin Upgrade to Support Windows 8.1 and Windows 2012R2

To install the Avaya ASGPlugin, you must have Microsoft .NET Framework 3.5 or later.

Additional Requirements to install and use ASG Plugin:

- Avaya ASGPlugin requires Administrative privileges to install.

- A reboot of the operating system after installation of ASGPlugin is required to complete the installation.

- From computer properties, clear **Allow connections only from computers running Remote Desktop with Network Level Authentication** check box.

Changing the font for Plain Text mode in Rich Client

Only three fonts for Plain Text mode in Rich Client by default are as follows:

- Serif

- Sans Serif

- Monospaced
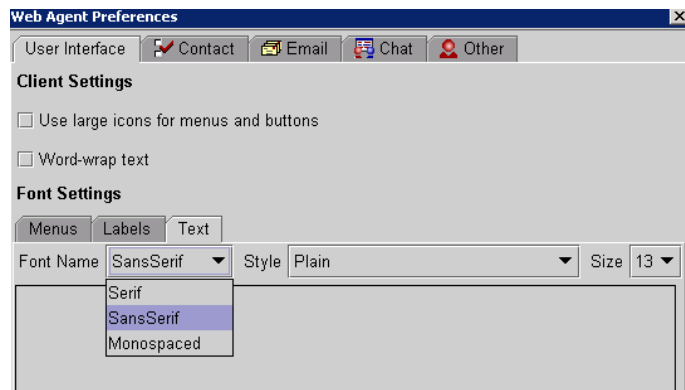
You can change the fonts in **Tools** > **Preferences** > **User Interface** > **Text**. To see the font name changing the Web agent must be reopened.

To add an additional font for Plain Text mode, you must do the following:

1. In `<Install dir>:\Avaya\WebAgent\` you make a folder, **Customization**. In the folder place the file PlainTextExtraFonts.properties.

2. Write down the list of necessary fonts to the file, for example:

   - Comic Sans MS

   - Tahoma

   - Times New Roman

3. Save file and re-login to Web Agent.

The list of font names from the file PlainTextExtraFonts.properties is added to the list of default font names in **Tools** > **Preferences** > **User Interface** > **Text**.

Performance upgrade of Poller and ICEmail Servers

In IC 7.3.3 FP, Poller server memory management has enhanced to avoid Poller crash issue for high email load. On Windows platform, functionality to monitor memory usage, Private Bytes for the Poller and ICEmail processes has been added.

Poller: When the upper threshold (configurable) is reached, Poller stops polling in new emails. As existing contacts are consumed, the memory usage decreases. When memory usage reaches the lower threshold (configurable), Poller starts polling emails again.

ICEmail: When the upper threshold (configurable) is reached, ICEmail stops fetching new email contacts from Poller. As existing contacts are consumed, the memory usage decreases. When memory usage reaches the lower threshold (configurable), ICEmail starts fetching email contacts again from Poller.

Refer "Configuration" section for configuration of the threshold values.

Enhancements in IC 7.3.2 Feature Pack

New Features and Enhancements

For more information, see "Avaya Interaction Center and Avaya Operational Analyst Overview and Specification" guide. This guide is available at http://support.avaya.com.

Security Enhancements

There are number of security enhancements introduced in IC 7.3.2 FP. Those are includes mainly –

- Preventing Cross-Site Scripting, mand-in-middle attacks
- Introduced "logout" option in IC Admin website
- Preventing arbitrary injection of JavaScript content
- Fixed Directory Traversal Vulnerability in HTTP Connector

For more information, see Avaya Interaction Center Release 7.3.x Security Guide. This guide is available at http://support.avaya.com.

Enhancements in IC 7.3.1 Service Pack

Overview of the Simplified IC Dump feature

In computing, a core dump consists of the recorded state of the available memory of a computer program at a specific time, when the program fails. The following other key pieces of the program state are also dumped simultaneously:

- The processor registers, which might include the program counter and stack pointer.

- The memory management information and other processor.

- The operating system flags and information.

Core dumps are useful debugging aids that can assist in diagnosing and debugging errors in computer programs. The following list displays some situations where core dumps are useful:

- A user can save a failures for later or offsite analysis, or for comparison with other failures.

- A user can capture data freed during dynamic memory allocation and might thus be used to retrieve information from a program that is no longer running.

- A programmer can use the core dump to determine the error from direct examination, in the absence of an interactive debugger.

A core dump represents the complete contents of the dumped regions of the address space of the dumped process. Depending on the operating system, the dump might contain few or no data structures to aid interpretation of the memory regions.
A debugger can use a symbol table or file to help the programmer in the following:
- Interpret dumps.

- Identifying variables symbolically.

- Displaying source code.

If the symbol table or file is unavailable, difficulty occurs to interpret the dump. Special-purpose tools called Dump Analyzers to analyze dumps are present.
If IC does not function according to the expected behavior, the reason might be incorrect implementation of business requirement or incorrect use of coding language and OS/Library APIs in the application code. Application logs help in troubleshooting the incorrect implementation of business requirement in the application code. For the other category, where incorrect application behavior is the result of incorrect use of coding language and OS/Library APIs, difficulty occurs to resolve the problem with the help of application logs only. Unavailability of the opportunities of live debugging on production system of the customer increases the problems. In such scenarios, core dump works as a critical aid to application log in finding the root cause of the issue. Postmortem debugging of core dumps helps in analyzing various application issues such as the following:
- Application crash analysis:

    - Access violation

    - Memory or Stack/Heap corruption

    - Stack overflow

- Memory, Resource or Handle leak analysis

- Hang analysis:

    - Low CPU hang

    - High CPU hang

- Inter process communication issues

The Simplified IC Dump feature helps IC processes to create core dump in various scenarios. The system automatically creates core dump in application failure scenarios. In other scenarios, where a process is still running, creating a core dump is similar to selecting the server in IC Manager, and then clicking a toolbar button.
Using the Simplified IC Dump feature, the IC Application can:
1. Create core dump with correct bitness, that is, 32-bit core dump.

2. Create full memory core dump file of the process.

3. Create core dump automatically on failure of any IC processes such as toolkit server or client.

---

4. Create core dump of a running IC Server through IC Manager without affecting the IC server process.

5. Create core dump at IC installation location, in the IC logs folder.

6. Create core dump with a unique name containing the time stamp so that earlier core dumps are preserved.

Note: The IC Dump feature is applicable to components that are compiled and maintained as part of the IC code. The IC Dump feature is not applicable to the components that are shipped and installed with IC, but not part of IC source code. For example, third party or Open Source components.

Installation and Configuration

Simplified IC Dump is installed by the installation of IC 7.3.1 or later service pack.
Most of the configurations for different IC flavors such as Design and Admin, Server, WebConnector, Clients running on different operating systems such as Windows, Solaris and AIX, is done automatically by the Service Pack installer.

IC WebServices service configuration for Windows platform

Perform the following steps on the computer where the IC WebServices service is configured for Windows:
1. Stop the IC WebServices service, if running.

2. Remove the already deployed IC WebServices service.

3. Deploy the IC WebServices service.

4. Start the IC WebServices service.

For more information, see Deploying Web Services chapter of the Installation and Configuration guide.
Note: You can also add the **-XX:+UseOSErrorReporting** JVM option in a new line to the following registry key:
- On a 64-bit Windows server:

  - ```
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software
    Foundation\Procrun 2.0\<IC WebServices Service
    Name>\Parameters\Java\Options
    ```

- On a 32-bit Windows server:

  - ```
    HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun
    2.0\<IC WebServices Service Name>\Parameters\Java\Options
    ```

Restart the WebServices service after adding the previous registry entry.

Core dump creation when IC process fails

A core dump generated in a fail scenario, with the right set of information contained in the core dump, is useful in finding the root cause of the coding issue through the postmortem debugging. The Simplified IC Dump feature performs the following:

- All IC processes such as a Toolkit server and client to create the full memory core dump file automatically at the IC install location.

- Names the core dump file using the component name and the time when the failure occurred.

Following is the core dump file naming convention in a fail scenario on different IC supported platforms:

- Crash dump on Windows platform

- Crash dump on Solaris platform

- Crash dump on AIX platform

Crash dump on Windows platform

The core dump for the Toolkit Server is created in `<AVAYA_IC73_HOME>\logs` folder with the name as `<ServerAlias>(<ExecutableName>)[PID]_Crash-<TimeStamp>.dmp`. For example, if an ADU Server with an alias name ADU_Voice1 and process id 1234 crashes at 11:23:45 AM on 01 March 2013, then the system creates in the `<AVAYA_IC73_HOME>\logs` folder the core dump file with name `ADU_Voice1(adusrv.exe)[1234]_Crash-20130301112345.dmp`.

The core dump for Toolkit Client is created in `<AVAYA_IC73_HOME>\logs` folder with the name as `<UserId>(<ExecutableName>)[PID]_Crash-<TimeStamp>.dmp`. For example, if the Avaya Agent Rich Client application with process id 2345 crashes at 10:39:56 AM on 01 March 2013 when Agent with login id agent1 was logged in, then the system creates in the `<AVAYA_IC73_HOME>\logs` folder the core dump file with name `agent1(qui.exe)[2345]_Crash-20130301103956.dmp`.

Note:
1. The TimeStamp is calculated using localtime_s API and will be in the format of YYYYMMDDHHMMSS.

2. The IC implemented unhandled exception filter hook code creates the core dump file. The code creates the core dump only for the scenario where the reason of crash is an unhandled exception in the code. This feature does not handle other reasons of crash. In other fail scenarios, you can use Windows Error Reporting or other similar methods and utilities for core dump creation.

3. To create a crash dump for Toolkit dependent IC components, running as snap-in within Microsoft Management Console ,mmc.exe, the following dialog box is displayed if the failure is within MM:

CRM Central Supervisor

MMC has detected an error in a snap-in. It is recommended that you shut down and restart MMC.

☐ Report this error to Microsoft, and then shut down MMC.

☑ Continue running and ignore errors with this snap-in for the rest of the session.

☐ Continue running and always ignore errors with this snap-in, regardless of user or session.

OK
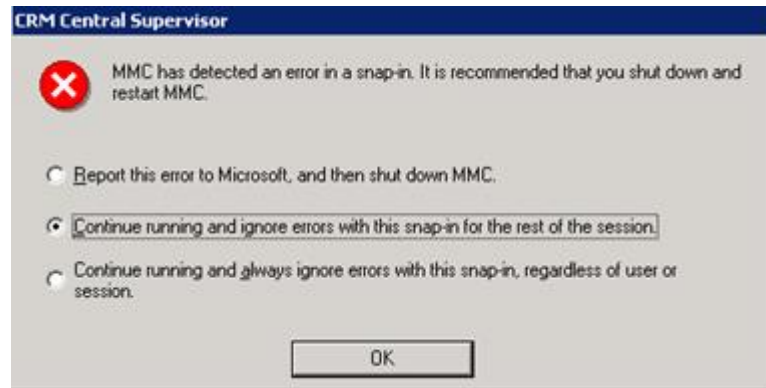
In the dialog box select the second option, **Continue running and ignore errors with this snap-in for the rest of the session**.

Crash dump on Solaris platform

The core dump of both, Toolkit Server and Toolkit Client, will be created at `<AVAYA_IC73_HOME>/logs` folder with the name as `<Executable Name>[PID]_Crash-<TimeStamp>.core`. For example, if ADU Server with an alias name ADU_Voice1 and process ID 1234 crashes at 11:23:45 AM on 01 March 2013, then the system creates in the `<AVAYA_IC73_HOME>\logs` folder the core dump file with the name `adusrv.exe[1234]_Crash-1362137025.core`. If Configuration Tool with process id 2345 crashes at 10:39:56 AM on 01 March 2013 when Administrator with the login id Admin was logged in, then the system creates in the `<AVAYA_IC73_HOME>\logs` folder the core dump file with the name `java[2345]_Crash-1362134396.core`.

Note: The TimeStamp is a decimal value of time(2) function. The time() function returns the value of time in seconds since 00:00:00 UTC, January 1, 1970. The Solaris OS creates the core dump file.

Crash dump on AIX platform

The core dump of both Toolkit Server and Toolkit Client is created in the current working folder of the process. Most of the current working folder of the IC process is either `<AVAYA_IC73_HOME>/etc` or `<AVAYA_IC73_HOME>/bin`.

The name of the core dump file is `core.PID.<TimeStamp>` if no JVM is loaded in the process memory irrespective of whether JVM is loaded explicitly or implicitly. In such a case, the AIX OS creates the core dump file. For example, if ADU Server with an alias name ADU_Voice1 and process ID 1234 crashes at 11:23:45 AM on 01 March 2013, then the system creates in the `<AVAYA_IC73_HOME>/etc` folder the core dump file with name `core.1234.01112345`.

The Time stamp is in the format of DDHHMMSS in the previous example.

The name of the core dump file is `core.<TimeStamp>.PID.<SequenceNo>.dmp` if JVM is loaded in the process memory. In such a case, the core dump creation for the process is controlled by JVM. For example, if Configuration Tool with process ID 2345 crashes at 10:39:56 AM on 01 March 2013 when the Administrator with login ID Admin was logged in, then the system creates in the `<AVAYA_IC73_HOME>/bin` folder the core dump file with name `core.20130301.103956.2345.0001.dmp`.

Note:

If the core dump creation is controlled by JVM, the time stamp is in the format of YYYYMMDD.HHMMSS. If JVM controls the core dump creation, JVM provides the SequenceNo.

Core dump creation of a running IC server

You can use the core dump of the process to troubleshoot some problems even though the process does not fail and is in a running state. Through postmortem debugging of core dump of the running application along with analyzing the application log you can rectify the following scenarios:

- Application freezing.

- Thread deadlock.

- Memory or handle leak.

Using the Simplified IC Dump feature, IC administrators can create core dump of any running IC server configured in IC Manager. You can create, through the IC Manager, the core dump of a running IC server by selecting single or multiple servers and clicking **Create server dump** on the Toolbar.
The core dump file of a running server is created in the `<AVAYA_IC73_HOME>/logs` folder on all three platforms. Following are the names of core dump files that the IC Manager creates on different platforms:

1. Windows: `<ServerAlias> [PID]_Dump-<TimeStamp>.dmp`

2. Solaris: `<ServerAlias> [PID]_Dump-<TimeStamp>.core.PID`

3. AIX: `<ServerAlias> [PID]_Dump-<TimeStamp>.core`

Note: The TimeStamp is calculated using localtime_s API on Windows and local time API on Solaris and AIX. The TimeStamp is in the format of YYYYMMDDHHMMSS.

Perform the following steps to create dump of a running IC server configured in IC Manager:

1. Log in to IC Manager using an account with Administrator privileges.

2. Select the server or multiple servers for creating the core dump.

3. Select one of the following methods to create a server dump:

   - From the **Create server dump** on the Toolbar as in the following image:

   - From the popup menu by right-clicking on the selected servers and selecting **Dump**.

   - From the Menu bar you select **Server**>**Dump**.

4. Select **Yes** in the confirmation dialog box.

The info alarm is displayed confirming successful creation of core dump of the selected servers. If a core dump is not generated successfully, the system displays a warning alarm.
IC Manager performs the following steps to internally create the core dump of selected servers:

1. IC Manager first pings the selected server by sending a Ping VESP request.

2. If the response to ping is successful, then IC Manager calls the Dump VESP method of the selected server.

3. If `Server.Ping` or `Server.Dump VESP` request fails, then IC Manager sends request to corresponding ORB server to create the core dump of the selected servers.

4. If the ORB is the parent process of the selected servers, then ORB creates core dump for that server. This process is a backup mechanism for creating core dump.

5. IC Manager raises an alarm notifying the success or failure of the core dump creation.

Note:
1. By launching a separate utility as a separate process and providing a process ID of the selected server as an argument to that utility process, you can create dump of a running server. The Simplified IC Dump feature uses `<AVAYA_IC73_HOME>\bin\avayadmp.exe`, gcore and gencore utilities for core dump creation on Windows, Solaris and AIX platforms respectively. Avayadmp.exe utility is a part of the IC 7.3.1 Service Pack. On Solaris and AIX, Avayadmp.exe is required to ensure that respective utilities, gcore and gencore are installed and the paths are resolved correctly.

2. The size of the Core dump is equivalent to the virtual memory size of the process at the time of dump creation. This size of core dump can vary from few hundred MBs up to 2 GB which is the user mode address space limit of any 32-bit process. Dump of a running process must not be created unnecessarily as it might consume disk space. An issue scenario must be considered and thought of. Contact Avaya support with the issue and the support team can advise you on how to take core dump for that particular issue and how many core dumps are required to take with what interval. Core dump of a running IC server must not be created without consulting Avaya support.

3. If an application fails the system creates an automatic Core dump creation. The issue, the core dump, and the application log file, must be reported to Avaya support. To speed up the resolution of the issue, provide the fail scenario and steps with the dump and log file.

Dump VESP request timeout setting

Timeout for Dump VESP request is configurable in server configuration through the DumpTimeout server configuration parameter. You can set this parameter between 20 to 160 seconds. The default value is 64 seconds. You can add the DumpTimeout parameter to the configuration tab of any server in IC Manager in the form of a new seqCouple.
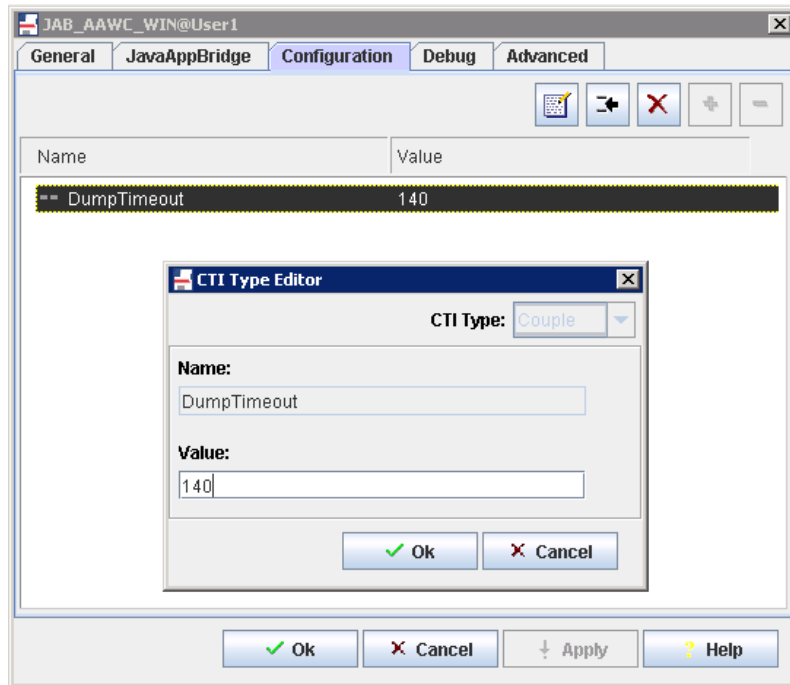
After adding or changing the DumpTimeout parameter in IC Manager, select **Server**>**Update** to start the parameter or value.

Note: This configuration parameter does not play any role in creating core dump because application crash. In most of the cases, you do not require to change the default DumpTimeout value for creating dump of a running IC server through IC Manager. You must add or change this configuration Avaya support recommends.

Creating dump with avayadmp application

If the system cannot create the dump of a running process through IC Manager on the Windows platform, then you can directly use the new avayadmp.exe application present in `<AVAYA_IC73_HOME>\bin` folder to create the dump through the command prompt. Avayadmp.exe can be used with the following command line arguments:

```
avayadmp.exe -p <Process Id> -t [Dump Type] -l [Dump Location] -n [Application Name] -d
[DbgHelp Library Path]
```

Command	Description
-p	Mandatory Parameter. Process ID of the application to be dumped.
-t	Optional Parameter. Type of dump. Values can be tiny, mini, midi, or full. If not provided, then the system creates a full dump.

Command	Description
-l	Optional Parameter. A valid dump location or folder where the system saves the dump. If the location or folder is not provided, then the system saves the dump in Windows Temp folder.
-n	Optional Parameter. Friendly application name. For example, alias name. If not provided, then the system uses the exe name to name the dump file.
-d	Optional Parameter. Valid folder of dbghelp.dll library. If not provided, then dbghelp.dll be tried first from folder of the application and then from Windows System folder.

Example: If the Avaya Agent Web Client process cannot process any VESP request, then the Client cannot create the dump of AAWC from the IC Manager Toolbar button, **Create server dump**. In such scenarios, the ORB server also does not help in creating the dump since the AAWC process is launched separately and is not managed by ORB process. In this case, avaydmp.exe can be directly used to create a dump of AAWC server by performing the following steps:

1. Get the process ID of AAWC, that is, javaw.exe using Windows Task Manager and note it down.

2. Open command prompt cmd.exe and navigate to `<AVAYA_IC73_HOME>\bin` folder.

3. Type the following command on the command prompt:

   ```
   avayadmp.exe -p <AAWC Process Id> -t full -l <AVAYA_IC73_HOME>\logs -n <AAWC
   server alias name> -d <AVAYA_IC73_HOME>\bin
   ```

4. Note the output of avayadmp.exe on command prompt and then check if the core dump file is at the specified location with the name as `<ServerAlias>[PID]_Dump-<TimeStamp>.dmp`.

Note: For other supported operating systems, such as Solaris and AIX, you can use the respective dump creation utilities to create the dump.

Operating System	Dump Creation Utility
Solaris	`gcore -o <AVAYA_IC73_HOME>/logs/<core dump file name> ProcessID`

Comments on this document? infodev@avaya.com

AIX	`gencore ProcessID <AVAYA_IC73_HOME>/logs/<core dump file name>`

For more information, see the respective platform manual.

Replace Workgroup Functionality

The Replace functionality is added to Multi Agent Edit feature of IC Manager. This functionality helps simplify the process of replacing the workgroup membership of an agent with new workgroup membership. This allows moving all agents of one workgroup to another workgroup.

In the Workgroup Membership window, a new button **Replace>>** was added.

Perform the following steps for the Replace operation:
1. User selects a workgroup membership from the **Member of** list on the right side.

2. User selects a replacement from **Workgroups** list on the left side.

3. User clicks **Replace>>**.
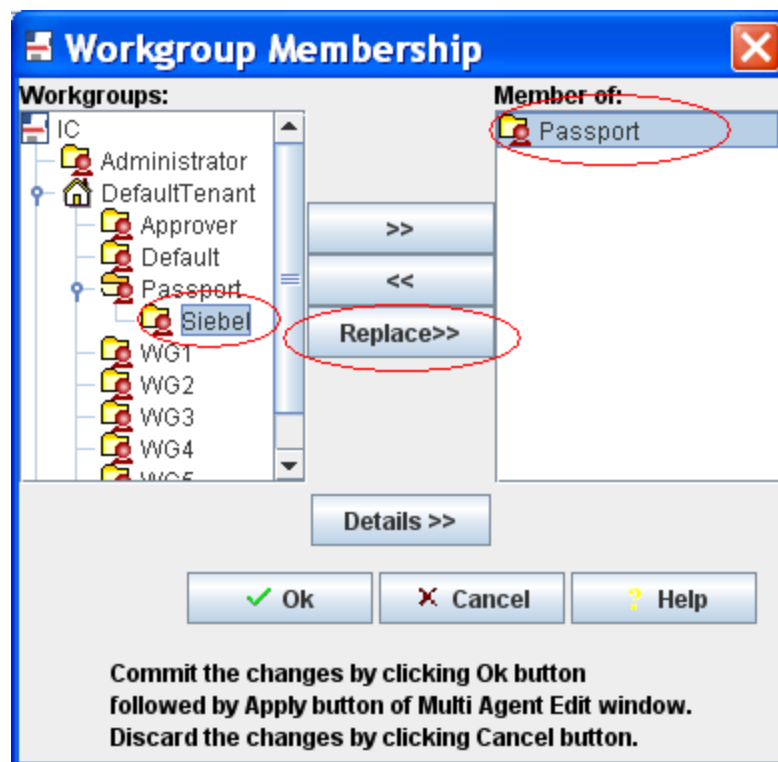
The scenarios with steps to perform the Replace operation are as follows:

Scenario 1:

All selected agents belong to only one workgroup and all agents must move to another workgroup.
For example, to move all agents from Passport workgroup to Siebel workgroup perform the following steps:
1. Select the original workgroup from the **Member of** list on the right side of the window.

2. Select the new workgroup from **Workgroups** list on the left side of the window.

3. Verify that all three buttons **>>** (Add), **<<** (Remove) and **Replace>>** are active.

4. Click **Replace>>** to move the agents from the original workgroup to the new workgroup.

5. Click **Ok** in the Workgroup Membership window.

6. Click **Apply** in the Multi Agent Edit window to commit the changes.

Because all agents belong to only one workgroup, the workgrouporder for all agents is zero. The database changes are shown in the following table:

Before performing Replace:

Agent	Workgroup	Value of the workgrouporder field in the groupmember table
agent1	Passport	0
agent2	Passport	0
agent3	Passport	0

After performing Replace:

Agent	Workgroup	Value of the workgrouporder field in the groupmember table
agent1	Siebel	0
agent2	Siebel	0
agent3	Siebel	0

Scenario 2:

The selected agents belong to multiple workgroups. You must replace one of the common workgroups that agents belong to with a new workgroup.

For example, to remove WG2 and replace WG2 with WG5 perform the following steps:

1. Select the original workgroup from the **Member of** list on the right side of the window.

2. Select the new workgroup from **Workgroups** list on the left side of the window.

3. Verify that all three buttons **>>** (Add), **<<** (Remove) and **Replace>>** are active.

4. Click **Replace>>** to move the agents from the original workgroup to the new workgroup.
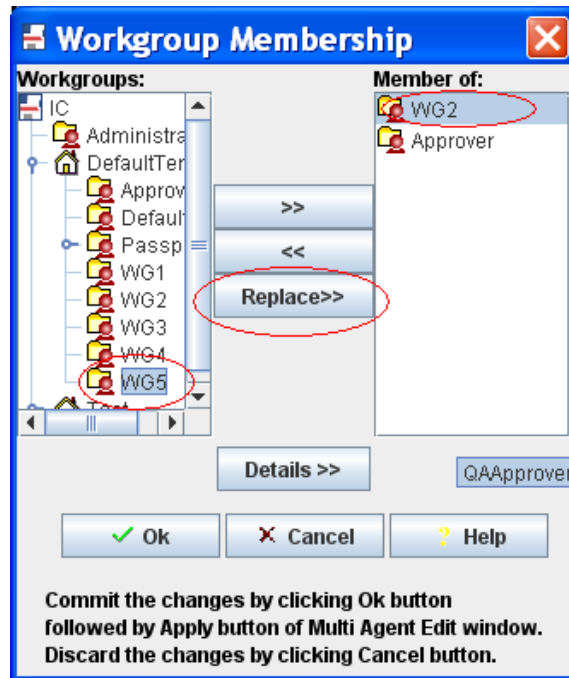
If some of the selected agents have the new workgroup as the primary workgroup, that is, workgrouporder for the workgroup is zero, the following message displays:
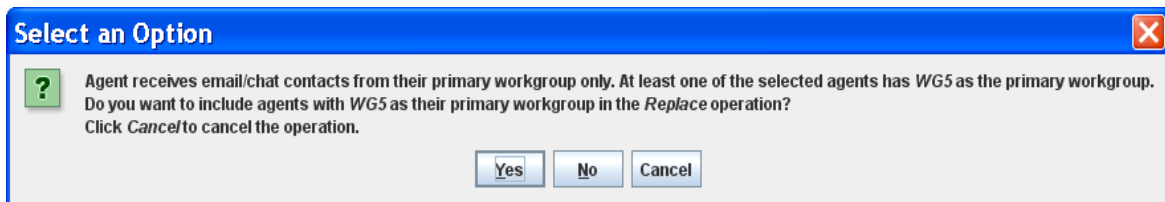
1. On selecting **Yes**, the system replaces the original workgroup with the new workgroup for all agents. The database changes after selecting **Yes** as follows:

Before performing Replace:

Agent	Workgroup	Value of the workgrouporder field in the groupmember table
agent1	Default	0
	WG2	1
	Approver	2
agent2	WG2	0
	Approver	1
agent3	WG5	0

Comments on this document? infodev@avaya.com

Agent	Workgroup	Value of the workgrouporder field in the groupmember table
	Approver	1
	WG2	2

After performing Replace:

Agent	Workgroup	Value of the workgrouporder field in the groupmember table
agent1	Default	0
	WG5	1
	Approver	2
agent2	WG5	0
	Approver	1
agent3	Approver	0
	WG5	1

2. On selecting **No**, the system skips the agents who have the original workgroup as the primary workgroup and then performs the replace operation for other selected agents. The database changes after selecting **No** as follows:

Agent	Workgroup	Value of the workgrouporder field in the groupmember table
agent1	Default	0
	WG5	1
	Approver	2
agent2	WG5	0
	Approver	1
agent3	WG5	0
	Approver	1
	WG2	2

3. To cancel the Replace operation select **Cancel**.

Other changes in the Agent Multi-Edit operation

1. Only one operation at a time:

   The user can perform only one operation, add, remove or replace, at a time. Before performing the next operation, the user must commit the changes by clicking **Apply** on the Agent Editor dialog box. Committing ensures that workgroup membership is up-to-date with proper ordering before the next operation, and avoids database corruption.

2. Display common members only:

   As the MultiEdit window displays common values across all agents being edited, only the common workgroups across all agents are displayed in the **Member of** field.

3. Adding new workgroup:

   If you add a new workgroup in the member of list, the workgroup is at the last position in the **Member of** list for each agent.

4. Removing workgroup from the list of common member:

   If you remove any workgroup from the **Member of** list then you remove the workgroup from all agents being edited. The order of the workgroups that is present after the workgroup being removed is pushed up by 1.

5. Workgroup reordering:

   Member reordering, that is, the member move-up and move-down arrow buttons are not available for MultiEdit, as the order of common groups might vary for all the agents being edited.

Chapter 3: IC 7.3.4 Installation

This section describes the SP Installer that updates the existing Avaya IC 7.3 systems with the Avaya IC 7.3.4 SP to provide fixes and enhancements for Avaya IC 7.3.

The Installation Tool performs the following steps:

1. Creates a backup of each file that the installer replaces with new files.

2. Copies the new IC 7.3.4 files into the appropriate folders on your system.

3. Creates the Uninstaller program.

4. Displays a screen that confirms a successful installation with the following text:

```
Installation was successful.

No errors or warnings were generated.

Complete log messages are available at:

.../IC73/ICServicePacks/7.3.4/<FolderNameOfComponent>/Log/install.log
```

`<FolderNameOfComponent>` is the folder name of each component where the respective component files are.

The Installation Tool provides a separate installation program for each IC component. The Installation Tool helps you to upgrade your computer based on the components that are running. The following table lists the name of the component and the respective folder name:

Component/computer	Folder Name
Administration and Design	DesignAdmin
Avaya Agent client	AvayaAgent
Avaya Agent Web Client	WebClient
Avaya Agent Web Client Connector	WebConnector
IC Servers	Server
Siebel Integration component (IC side)	ICSideSiebel
Siebel Integration component (Siebel side)	SiebelSideIC

For Windows installations, the Installation Tool also:

1. Unregisters the necessary files on your system.

2. Registers the new files on your system.

Before you install

You must have separate computers for each IC component. Avaya does not support multiple IC components installed on the same computer. The following is a list of all IC components:

- IC Servers

- Avaya Agent

- Avaya Agent Web Client Connector

- Administration and Design

- Siebel Integration component [IC side]

- Siebel Integration component [Siebel side]

- SDK

Also ensure that no instance of Tomcat and JRE are running.

Note: If you are installing an IC on a fresh system using the RTM installer, then some error messages can popup during the installation of the SP. These error messages state that the file being copied during the SP installation is older than the file that already exists on the system. This is a valid scenario, and the customer must replace the existing files with the files being copied by the SP installer.

When installing IC using the RTM installer, the installer adds data about the installation location of IC to some of the files that the installer is installing. Due to this, the modification time of the file changes to the current time. If the IC system was installed during the development phase or after the release of the SP, then it might happen that some of the files in the SP have a modification time that is earlier than those of the same files installed on the system. This change is due to the RTM installer modifying the files.

In such cases, the message, as described earlier, pops up during the SP installation. You can ignore the error message and continue with the installation by choosing **Replace** on the dialog box that pops up.

Carefully review the installation instructions and also the list of files being installed from every package. The files which are part of the SP will replace the existing files on the system. If the current installation at the customer site involves configuration changes or customization, backup the original files in a separate folder to identify the old configuration or customization content. After the installation is successful, review the content of the newly installed files and merge the previous configuration or customization. Do not replace the new file with the old one directly as it might result in loss of new content.

Ensure your system conforms to the prerequisites. For more information see *IC 7.3.x Prerequisite guide.*

Ensure that you have a IC system of 7.3.x with valid License before proceeding.

Stop Avaya Agent Web Client

Before you run the IC 7.3.4 installation, you must stop the Avaya Agent Web Client. Ensure that all IC Avaya Agent Web Clients are logged off prior to stopping the Avaya Agent Web Client.

On the Avaya IC 7.3 release, you can start and stop the Avaya Agent Web Client component by stopping the javaw process.

To stop the javaw process perform the following:

1. For Windows operating system, click **Start** > **Run** to open the command prompt.

2. Change the folder to: `AVAYA_IC73_HOME\IC73\bin`.

3. Run the following command:

Operating System	Procedure
Windows	To stop: aawcclient.bat stop
Solaris	To stop: ./aawcclient.sh stop

Stop IC services

Before you run the IC 7.3.4 Server installation, you must stop all IC services and ensure those services are stopped. This might take several minutes because then the servers can complete their current tasks before shutting down.

Windows

To stop the IC Services perform the following:

4. Click **Start** > **Run**.

5. In the Run box, type `services.msc`, and press **Enter**.

6. Stop the following services. Some of these services might not exist on every IC server:

   - Avaya IC CIRS Service 7.3

   - Avaya IC Email Template Management Service 7.3

   - Avaya ICM Service 7.3

   - Avaya IC ORB Service 7.3

- Avaya IC Test Service 7.3

- Avaya IC Web Management Service 7.3

- Avaya IC WebLM Service 7.3

- Avaya IC CSPortal Web Service 7.3

- Avaya Voice Media Manager

- Avaya SDK Services

- Avaya Business Advocate Component Manager

Solaris

To stop the IC Services perform the following:

1. Log in with root privileges and navigate to `../IC73/bin` folder:

2. For ICM, at the command prompt, type: `./icm.sh stop –force`, and press **Enter**.

3. For CIRS, at the command prompt, type: `./cirs.sh stop –force`, and press **Enter**.

4. To stop multiple Tomcat instances, at the command prompt, type: `./ictomcat.sh stop all –force`, and press **Enter**.

5. To stop a single Web Application, at the command prompt, type: `./ictomcat.sh stop <servicename> -force`, and press **Enter**.

For oracle iplanet server, perform the following:

1. Go to the `<Oracle-iPlanet-Web-Server_HOME>/<https-node-name>/bin/` path.

2. Type: `./stopserv`.

3. Press **Enter**.

4. Go to `<Oracle-iPlanet-Web-Server_HOME>/admin-server/bin/` path.

5. Type: `./stopserv`.

6. Press **Enter**.

Stop IC servers

Before you run the IC 7.3.4 Server installation, you must stop all IC servers and all processes. Ensure that all IC Avaya Agents and IC Avaya Agent Web Clients are logged off prior to stopping all IC servers. This might take several minutes because the servers must complete their current tasks before shutting down.

You can stop IC servers on any of the supported platforms using either IC Manager or the Avaya IC Admin Utility.

Windows

IC Manager

To stop all IC servers in the proper order using IC Manager, perform the following:

1. Start IC Manager, if application is not already running.

2. Click the **Server** tab.

3. Select **Server** > **Shutdown**.

4. Select the IP address or the name of the computer on which you want to stop servers.

5. Click **OK**.

Avaya IC Admin Utility

To stop all IC servers using the Avaya IC Admin Utility on the IC server computer, perform the following:

1. In a command window, navigate to the `...\IC73\bin` folder.

2. Stop all IC servers, perform the following:

   ▪ To stop IC servers on all/multiple computers (multibox setup):

At the command prompt, enter the command: `icadmin tva <username> <password>`.

Press **Enter**.

   ▪ To stop IC servers on one system, perform the following:

      2. At the command prompt, enter the command: `icadmin tv <username> <password>`.

      3. Press **Enter**.

Note: Ensure that the login credentials used in the IC Admin Utility command have IC administrative privileges.

Advocate Servers and Administration

Perform the following steps on each Advocate Administration and Server computer:

1. Close Advocate Administration.

2. Click **Start** > **All Programs** > **Administrative Tools** > **Component Services**.

3. In **Component Services**, click **Computers** > **My Computer** > **COM+ applications** > **Avaya Business Advocate**.

4. Right-click the package and select **Shutdown**.

Solaris, AIX and Linux

IC Manager

Perform the following steps to stop all IC servers in proper order using IC Manager:

1. Start IC Manager, if application is not already running.

2. Click the **Server** tab.

3. Click **Server** > **Shutdown**.

4. Select the IP address or the name of the computer on which you want to stop servers.

5. Click **OK**.

Avaya IC Admin Utility

Perform the following steps to stop all IC servers, including the ORB server, using the Avaya IC Admin Utility on the IC server computer:

1. In a command window, navigate to the `.../IC73/bin` folder.

2. Stop all IC servers:

   ▪ To stop IC servers on all/multiple computers (multibox setup), perform the following:

      1. At the command prompt, enter the command: `./icadmin tva <username> <password>`.

      2. Press **Enter**.

   ▪ To stop IC servers on one computer, perform the following:

      3. At the command prompt, enter the command: `./icadmin tv <username> <password>`.

      4. Press **Enter**.

Note: Ensure that the login credentials used in the IC Admin Utility command have IC administrative privileges.

Ensuring all IC servers and services are stopped

Windows

1. Go to the Task Manager dialog box.

2. Click the **Process** tab to view a list of the processes on your computer.

3. Check to ensure the IC servers are not running.

Solaris, AIX and Linux

4. At the command prompt, type the following command:

    ```
    ps -ef | grep <AVAYA_IC73_HOME>/bin | grep -v grep
    ```

5. Press **Enter**. This command displays a list of processes related to IC servers.

6. Ensure the IC servers and any processes are not running.

7. To stop multiple processes with one command, type the following command:

    ```
    kill -9 <PID>
    ```

    Where **<PID>** is the Process ID of each process that is related to IC servers.

Note: You can also type `kill -9 <PID1> <PID2>.... <PIDn>` to end all the processes with a single command.

8. Press **Enter**.

Backup configuration files

If you are upgrading existing IC 7.3.x setup, then following configuration files need to be backed up.

sc.xml
If you have performed any customization in the existing `sc.xml` file, then you must take the backup of this file. This file is located on the machine where Design and Admin is installed. The file location is `<AVAYA_IC73_HOME>\etc\sc.xml`. Take the backup of this file before proceeding further installation.

AARC Scripts
If you have changed any AARC scripts, then you must take the backup of such files. These files are located on the machine where Design and Admin is installed.

For example if you have changed `CoreServices_Login.qsc` file, then back up the file `<AVAYA_IC73_HOME>\design\QConsole\CoreServices_Login.qsc` and store this file to some other backup location.

Certificate Files
If you have configured HTTPS, then rake the backup of certificates files. For example, keystore and .cer files in `AVAYA_IC73_HOME\Java\lib\security` folder.

WebLM Files
Take the backup of files as described in the following table:-

File/Folder	File Location	Required	Description

File/Folder	File Location	Required	Description
Users.xml – File	<AVAYA_IC73_HOME>/tomcat/webapps/WebLM/admin	Yes, if any users are added that are to be retained.	This file contains the list of users.
Product_folder – Folder	<AVAYA_IC73_HOME>/tomcat/webapps/WebLM/data/	Yes	The product folder that contains the configuration files. For example, aic.
License file (.xml) – File	<AVAYA_IC73_HOME>/tomcat/webapps/WebLM/licenses	Yes	The installed license file
usagehistory.properties – File	<AVAYA_IC73_HOME>/tomcat/webapps/WebLM/data	Yes	The Usage History Information
weblmserver.properties – File	<AVAYA_IC73_HOME>/tomcat/webapps/WebLM/data	Yes, if WebLM configuration properties have been modified	The server properties file.

And then delete the `<AVAYA_IC73_HOME>/tomcat/webapps/WebLM` folder

vesp.imp and ds.ffd

Take the backup of `vesp.imp` and `ds.ffd` files from the Primary IC Server machine. These files are located in `<AVAYA_IC73_HOME>\etc` directory. These are important files which are helpful in restoring a setup.

Prerequisites

Prerequisites for running config tool in IC 7.3.4

1. Focus related issues have been observed with Config Tool when using X-Servers like MobaXterm, X-ming or others. It is recommended to use the Cygwin/X server in the "Windowed or rooted mode" which do not exhibit these issues.

2. Please also ensure that the Cygwin/X server is listening on TCP socket as well. Refer "Config Tool" subsection in "Chapter 7: Troubleshooting" section from the List of Fixed Issues, Known Issues, and Troubleshooting for Avaya IC 7.3.x document for more details..

Prerequisites for Launching AAWC in IC 7.3.4

Following are the prerequisites for AAWC -

- AAWC launch machine should have 32 bit JRE 1.8.0.40 or higher version of 1.8
- Only one instance of JRE should be installed and enabled.

Prerequisites for installing IC 7.3.4

This section describes the prerequisites for installing the IC 7.3.4 Service Pack.

1. Before you install IC 7.3.4, you must have IC 7.3 installed on your system. IC 7.3.4 upgrade is also supported from IC 7.3.1 SP or IC 7.3.2 FP or IC 7.3.3 FP.

Getting Started

Avaya IC 7.3.4 is available on the Avaya Support Web site at: http://support.avaya.com/downloads/

To receive the IC 7.3.4 release on a CD, send an email requesting the media (CD) to icoakeyrequest@avaya.com with the following details:

- Customer Name

- Avaya Sold-to Number

- Contact Name

- Contact Address

- Contact Phone Number

- What CDs you are requesting

Obtaining a License Key

Avaya Interaction Center (IC) and Avaya Operational Analyst (OA) are enabled for run-time operation with a license key that provides features and capacity based on your specific order. The following information assists you in requesting your license keys.

If you have a valid license key and then move to a newer IC and OA release from an earlier release, your license key continues to be valid. It contains the IC and OA features and capacity you are entitled to with your software licensed from Avaya. Unless you have made changes that modify your HostID on the server where the license manager is operating, you do not need a new license. For Windows deployments of WebLM, the license is keyed on the MAC address of the server, not the HostID.

Creating License Request

Perform the following steps to create the license request:

1. License Key Request (New)

   Send to: icoakeyrequest@avaya.com

   Provide the following details:

   - Customer Name.

   - Customer Location (city, state, country).

   - Avaya SAP Order Number.

   - MAC Address (HostID for Solaris) of all Servers running WebLM Service.

   - System Purpose (for example, Production, Test, Lab).

   - Return Email address.

   - Implementer of system (Avaya PSO, Avaya Business Partner, or SI, self).

2. License Key Request (Addition/change)

   Send to: icoakeyrequest@avaya.com

   Provide the following details:

   - COPY OF CURRENT LICENSE FILE (IMPORTANT)

   - Customer Name.

   - Customer Location (city, state, country).

   - If adding - Avaya SAP Order Number.

   - Avaya Customer Number.

   - If changing - MAC Address (HostID for Solaris) of all Servers running WebLM Service.

   - System Purpose (for example, Production, Test, Lab).

- Return Email address.

- Implementer of system (Avaya PSO, Avaya Business Partner, or SI, self).

Downloading the IC 7.3.4 Feature Pack

You can download the IC 7.3.4 Service Pack files from the Avaya Support site:
http://support.avaya.com/downloads/.

To download IC 7.3.4, perform the following:

1. On the Avaya support site, click **Downloads & Documents** menu.

2. In the **Enter Your Product Here** field, enter the product name **Interaction Center**.

3. Click the **Choose Release** drop-down list and select 7.3.x.

4. Select **Downloads**.

5. Click **Enter**.

6. Click the appropriate IC 7.3.4 file name to download the respective file.

7. Move the IC 7.3.4 files to an installation folder on the system where you want to store them.

Note: The name of the installation folder can contain only acceptable characters, such as A-Z, a-z, 0-9, -, and
_, for the installation to run successfully. The Installation wizard does not copy files from a folder that contains
any other special characters in its name.

Installation files

The following table indicates the computer type, operating system, and the file name for each of the IC 7.3.4
components:

Note: The mapped network drive installation option is unavailable for the Solaris, AIX and Linux platforms.

Component/computer	Operating System	File name
Administration and Design	Windows	`IC734WinAdmin.zip`. Extract the files into the install folder on the local computer or on the mapped network drive, depending on the installation option you want to follow.
Avaya Agent client	Windows	`IC734WinAgentClient.zip`. Extract the files into the install folder on the local computer or on the mapped network drive, depending on the installation option you want to follow.
Avaya Agent Web Client	Windows	`IC734WinWebClient.zip`. Extract the files into the install folder on the local computer or on the mapped network drive, depending

Component/computer	Operating System	File name
		on the installation option you want to follow.
Avaya Agent Web Client Connector	Windows	`IC734WinWebConnector.zip`. Extract the files into the install folder on the local computer or on the mapped network drive, depending on the installation option you want to follow.
	Solaris	`IC734SolWebConnector.tar`. Extract the files into the install folder on the local computer.
IC Servers	Windows	`IC734WinServer.zip`. Extract the files into the install folder on the local computer or on the mapped network drive, depending on the installation option you want to follow.
	Solaris	`IC734SolServer.tar.` Extract the files into the install folder on the local computer.
	AIX	`IC732AixServer.tar`. Extract the files into the install folder on the local computer.
Siebel Integration component (IC side)	Windows	`ICSide734win.zip`. Extract the files into the install folder on the local computer or on the mapped network drive, depending on the installation option you want to follow.
	Solaris	`ICSide734SolServer.tar.` Extract the files into the install folder on the local computer.
	AIX	`ICSide734aix.tar`. Extract the files into the install folder on the local computer.
	Linux	`ICSide734Linux.tar.` Extract the files into the install folder on the local computer.
Siebel Integration component (Siebel side)	Windows	`SiebelSide734win.zip`. Extract the files into the install folder on the local computer or on the mapped network drive, depending on the installation option you want to follow.
	Solaris	`SiebelSide734SolServer.tar.` Extract the files into the install folder on the local computer.
	AIX	`SiebelSide734aix.tar`. Extract the files into the install folder on the local computer.
	Linux	`SiebelSide734Linux.tar.` Extract the files into the install folder on the local computer.
IIS	Windows	`IC734WinIIS.zip` Extract the files into the install folder on the local computer or on the mapped network drive, depending on the

Component/computer	Operating System	File name
		installation option you want to follow.

Installation options

Avaya IC 7.3.4 provides the following installation options:

- Network installation with mapped drive

- Local installation

- Silent installation

- Console installation

The following components are installed on the Windows, Solaris, AIX and Linux operating systems:

- IC Server components.

- Siebel Integration component [Siebel side].

- Siebel Integration component [IC side].

The following components are installed on the Windows and Solaris operating systems:

- Avaya Agent Web Client Connector.

All other components are installed on the Windows platform only.

For more information, see IC 7.3 Installation Planning and Prerequisites.

Network installation with mapped drive

You can install IC 7.3.4 from a shared network computer to upgrade other computers without having to copy the IC 7.3.4 files from the central computer to those computers.

To enable your local computer to access the network computer, you must map a drive from the local computer to the network computer by selecting the **Tools** > **Map Network Drive** in Windows Explorer.

Note: If Universal Naming Convention (UNC) is not supported, you must map the drive to be accessed from the installation computer. UNC specifies a common syntax for accessing network resources, such as shared folders and printers.

For example, the syntax for Windows systems is as follows: `\\computername\sharedfolder\resource`.

Local installation

To install on local computers, copy the component folder, for example, Server, Avaya Agent, or Avaya Web Agent Client from the central computer to the computer where you want to install the component.

Silent installation

When you run installation in silent mode, the user interface is unavailable. To run the installer in the silent mode, a response file is required. The response file can be created by running the installer in record mode. The options selected during the recoding mode will apply when running the installer in the silent mode.

Record mode

In record mode, the installer runs the installation normally but records all of your inputs in a text file.

To run the installer in record mode, perform the following:

1. Go to the package folder where the contents of the FP installer are extracted.

2. At the command prompt, type:

    `<setupfile> -options-record <AbsolutePathOfFile.ext>`

For example:

Operating System	Command
Windows	`setupwin32.exe -options-record "D:\temp\SPSilent.opt"`
Solaris	`./setupsolarisSparc.bin -options-record "/tmp/SPSilent.opt"`
AIX	`./setupaix.bin -options-record "/tmp/SPSilent.opt"`

Linux	`./AICLinux -r /tmp/LSPSilent.opt`
	
	`./SiebelLinux -r /tmp/SSPSilent.opt`

Note: The `<setupfile>` is the operating system specific name of the setup executable and `<AbsolutePathOfFile.ext>` is the qualified file name. The `AbsolutePathOfFile` is the name of the file and `ext` is the file extension.

3. Press **Enter**.

    The installer creates the `<AbsolutePathOfFile.ext>` file containing all of your inputs.

Silent mode

In a silent mode, rerun the same installation on another system using the inputs from the text file.

To rerun the installer in silent mode:

1. Copy the `<AbsolutePathOfFile.ext>` file to the computer where you are to install.

2. Go to the package folder where the contents of the Feature Pack installer are extracted.

    At the command prompt, type:

    `<setupfile> -options <AbsolutePathOfFile.ext> -silent`

For example:

Operating System	Command
Windows	`setupwin32.exe -options "D:\temp\SPSilent.opt" -silent`
Solaris	`./setupsolarisSparc.bin -options "/tmp/SPSilent.opt" -silent`
AIX	`./setupaix.bin -options "/tmp/SPSilent.opt" -silent`

Linux	`./AICLinux –i silent –f /tmp/LSPSilent.opt`
	
	`./SiebelLinux –i silent –f /tmp/SSPSilent.opt`

Note: The `<setupfile>` is the operating system specific name of the setup executable and `<AbsolutePathOfFile.ext>` is the qualified file name. The `AbsolutePathOfFile` is the name of the file and `ext` is the file extension.

3. Press **Enter**.

    The installer creates the `<AbsolutePathOfFile.ext>` file containing all of your inputs.

Console installation

When you run installation in console mode, the user interface is not available.

To run the installer in console mode you enter the following command at the command prompt:

`<setupfile> -console`

For example:

Operating System	Command
Windows	`setupwin32console.exe -console`
Solairs	`./setupsolarisSparc.bin -console`
AIX	`./setupaix.bin –console`

Linux	`./AICLinux.bin –console`
	
	`./SiebelLinux.bin -console`

Note: The console option can be used for installation and uninstallation of all components.

Order of installation

After you complete the instructions for a network installation or a local installation, install the IC 7.3.4 components in the following order:

Note: The console option can be used for installation and uninstallation of all components.

- Server installation
- Siebel Integration Component installation
- Avaya Agent Web Client Connector installation
- Avaya Agent Web Client installation
- Administration and Design installation
- Avaya Agent (rich client) installation

Server installation

This section describes the installation procedures for the IC 7.3.4 Server component. The Server component can be installed on the Windows, Solaris and AIX platforms.

This section includes the following topics:

- Windows installation procedures

- Solaris installation procedures

- AIX installation procedures

Note: The files for SDK components are currently bundled with the IC Servers installation package for the Windows, Solaris, and AIX platforms. If you have IC setup as a multi-box setup such as, primary computer, secondary computer, and so on, you must install the IC Servers setup on all these computers.

Windows installation procedures

Perform the following steps on the Windows computers running the IC servers:

1. Before you begin the FP Installation, ensure that all IC components are stopped as explained in the sections, Stop IC servers and Stop IC services.

2. Go to the folder where you extracted the contents of the `IC734WinServer.zip` file.

3. Copy the IC734WinServer folder to the computer where you want to install the Server component. If you are accessing a network computer through a mapped drive, you do not need to copy the folder. Perform the following steps from your server:

   a. Open the IC734WinServer folder and double-click `setupwin32.exe` to start the installation program.

   b. At the Welcome screen, click **Next**.

   c. The next screen displays the location of the Uninstall program, click **Next**.

   d. In the dialog box that prompts **Please stop all Avaya IC servers and services**, click **Continue**.

   e. The next screen displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

1. Creates a backup folder and moves the existing server files to that folder.

2. Copies the new server files to the proper folders.

3. Registers the new .ocx and .dll files.

4. Installs the Uninstall program.

5. Displays the results of the installation:

If installation is successful, the system displays:	If installation is unsuccessful, the system displays:
Installation was successful. No errors or warnings were generated. Complete log messages are available at: ...\IC73\ICServicePacks\7.3.4\Server\Log\install.log	ALERT! Installation failed. Please fix these errors and re-run the installer. The following errors or warnings were generated. Complete log messages are available at: ...\IC73\ICServicePacks\7.3.4\Server\Log\install.log LIST OF ERRORS AND WARNINGS

6. Click **Finish**.

7. If the installation is unsuccessful, run the Uninstall program. Correct the errors and re-run the Installation program.

8. If a Telephony Server is configured, go to the `AVAYA_IC73_HOME\bin` folder and delete the `tssrv.exe` and `tssrv.pdb` files. Now perform the following copy/rename operation for supported IC switches

Switch	Copy...	Rename to...
Avaya DEFINITY/CM	cvlansrv.exe, cvlansrv.pdb	tssrv.exe, tssrv.pdb

9. If a TSQS Server is configured, go to the `AVAYA_IC73_HOME\bin` folder and delete the `tsqssrv.exe` and `tsqssrv.pdb` files. Now perform the following copy/rename operation for supported IC switches

Switch	Copy...	Rename to...
Avaya DEFINITY/CM	tsqssrv_asai.exe, tsqssrv_asai.pdb	tsqssrv.exe, tsqssrv.pdb

10. On the Web Management Services IC computer, delete the folder **localhost** from `<AVAYA_IC73_HOME>/IC73/tomcat/work/Catalina/`.

11. If the installation is successful, reboot the computer before you restart the servers.

Note: In September 2012, Avaya has announced End of Sale (EoS the support of Avaya IC support for third-party switches (PABXes) vide End of Sale Notice. You can view this announcement from the following location: https://downloads.avaya.com/css/P8/documents/100166179. As noted in the EoS notice, the End of Manufacturing Support for third-party switches is effective from December 2013. For more information, see the End of Sale Notice.

Solaris installation procedures

To run the Solaris installer, you must log in with root privileges. Perform the following steps on the Solaris computers running IC servers:

1. Before you begin the FP Installation, ensure that all IC components are stopped as explained in the sections, Stop IC servers and Stop IC services.

2. Go to the folder where you uncompressed the contents of the `IC734SolServer.tar` file.

3. At the command prompt, type: `$AVAYA_IC73_HOME/bin/icenv ./setupsolarisSparc.bin`.

   The `$AVAYA_IC73_HOME/bin/icenv` sets the IC environment variables and `./setupsolarisSparc.bin` starts the Server installation.

4. On the Welcome screen, click **Next**.

5. The next screen displays the location of the Uninstall program, click **Next**.

6. In the pop-up window that prompts: **Please stop all Avaya IC servers and services**, click **OK**.

7. The next screen displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

1. Creates a backup folder and moves the existing server files to that folder.

2. Copies the new server files to the proper folders.

3. Installs the Uninstall program.

4. Displays the results of the installation.

If installation is successful, the system displays: Installation was successful. No errors or warnings were generated. Complete log messages are available at: .../IC73/ICServicePacks/7.3.4/Server/Log/install.log	If installation is unsuccessful, the system displays: ALERT! Installation failed. Please fix these errors and rerun the installer. The following errors or warnings were generated. Complete log messages are available at:

	.../IC73/ICServicePacks/7.3.4/Server/Log/install.log
	LIST OF ERRORS AND WARNINGS

5. Click **Finish**.

6. If the installation is unsuccessful, run the [Uninstall program](#). Correct the errors and rerun the Installation program.

7. If the tssrv file exists on the system, check to see if this file is a symbolic link to the Telephony Server executable.

   At the command prompt, type `ls -l tssrv`.

8. If the tssrv is a symbolic link to the Telephony Server, the system displays: `lrwxrwxrwx filenameA -> filenameB`. The `filenameA` is a variable for tssrv and `filenameB` is the absolute server name.

9. If the tssrv file is a symbolic link to the Telephony Server, use the existing file without renaming it.

Switch	Use
Avaya DEFINITY/CM	cvlansrv

10. If the tssrv file is not a symbolic link to the Telephony Server, take a backup of the tssrv file, and delete the file from its current location. Make a copy of the file for your switch and rename the copy to tssrv.

    For example: For Avaya DEFINITY/CM, create a copy of cvlansrv and rename it as tssrv in the `AVAYA_IC73_HOME/bin` folder.

Switch	Copy...	Rename to...
Avaya DEFINITY/CM	cvlansrv	tssrv

11. If a TSQS Server is configured, take the backup of the tsqssrv file, and delete the file from its current location. Make a copy of the file for your switch and rename the copy to tsqssrv.

    For example: For Avaya DEFINITY/CM, create a copy of tsqssrv_asai and rename it as tsqssrv in the `AVAYA_IC73_HOME\bin` folder.

Switch	Copy...	Rename to...
Avaya DEFINITY/CM	tsqssrv_asai	tsqssrv

12. Backup the qorasrv file from the `..\IC73\bin folder`.

Note:

- If you are using an Oracle 10 DB Client, rename qora10srv as qorasrv in the `..\IC73\bin` folder.

- If you are using an Oracle 11 DB Client, rename qora11srv as qorasrv in the `..\IC73\bin` folder.

- On the Web Management Services IC computer, delete the folder **localhost** from `.../IC73/tomcat/work/Catalina/`.

Execute this step on only the Web Management Services IC system.

AIX installation procedures

Before running the SP installer on the AIX platform, you must end the processes that use the Rogue Wave binary files installed on the system.

Note: IBM AIX is only supported on Interaction Center Release 7.3, 7.3.1, and 7.3.2. For more information see the Supported Server Operating Systems section in the *Avaya IC Installation Planning and Prerequisites Guide*.

AIX installation prerequisites

Perform the following steps before carrying out the installation on the AIX platform:

a. Ensure that all IC components are stopped as explained in the sections, Stop IC servers and Stop IC services.

a. Change the directory to $AVAYA_IC73_HOME/lib.

b. At the command prompt, type: **slibclean**

c. At the command prompt, type: **fuser -k lib*12d*.a**

Note: After running the fuser -k lib*12d*.a command, type the following at the command prompt:

fuser lib*12d*.a

d. At the command line, type the command: fuser -k lib*.so

Note: After running the fuser -k lib*.so command, type the following at the command prompt:

fuser lib*.so

No process IDs should be displayed in the results after running this command. However, if any process ID is displayed in the results, restart the AIX machine.

e. After performing the steps, proceed with the installation on the AIX platform.

AIX installation

Perform the following steps on the AIX machines running the IC servers.

Note: To have the permissions to run the AIX installer, you must log in with root privileges.

a. Before you begin the FP Installation, ensure that all IC components are stopped as explained in the sections, Stop IC servers and Stop IC services.

b. Go to the directory where you uncompressed the contents of the IC732AixServer.tar file.

c. At the command prompt, type:

   export AVAYA_IC73_HOME=<Avaya IC Servers installation path>

   For example, **export AVAYA_IC73_HOME=/opt/Avaya/IC73**

d. Press **Enter**.

e. At the command prompt, type: **$ ./setupaix.bin**.

f. On the Welcome screen, click **Next**.

g. On the next screen, which displays the location of the Uninstall program, click **Next**.

h. In the pop-up window that prompts Please stop all Avaya IC servers and services, click **OK**.

i. On the next screen, the system displays the installation summary, click **Next** to run the installation. The Installation Tool performs the following:

   ▪ Creates a backup directory and moves the existing server files to that directory.

   ▪ Copies the new server files to the proper directories.

   ▪ Installs the Uninstall program.

   ▪ Displays the results of the installation.

If installation is successful, the system displays:	If installation is unsuccessful, the system displays:
Installation was successful. No errors or warnings were generated. Complete log messages are available at: .../IC73/ICServicePacks/7.3.2/Server/Log/install.log	ALERT! Installation failed. Please fix these errors and re-run the installer. The following errors or warnings were generated. Complete log messages are available at: .../IC73/ICServicePacks/7.3.2/Server/Log/install.log

LIST OF ERRORS AND WARNINGS |

j. Click **Finish**.

k. If the installation is unsuccessful, run the Uninstall program. Correct the errors and re-run the Installation program.

Siebel Integration Component installation

This section describes the installation procedures for the Siebel Integration Component of the Avaya IC 7.3.4 release. The Siebel Integration component is installed on the Windows, Solaris, and AIX computers running

Siebel Services and Avaya IC servers. Install the Siebel Integration component only when your IC system is integrated with Siebel.

The Siebel section includes the following topics:

- Windows installation procedures

- Solaris installation procedures

- AIX installation procedures

Windows installation procedures

You must install the Siebel Integration component on the computer running Siebel Services and the computer running IC servers.

Siebel Integration component on Siebel server

Perform the following steps on the Windows computers that are running Siebel Services:

1. Go to the folder where you extracted the contents of the `SiebelSide734win.zip` file.

2. Open the SiebelSide734win folder and double-click on setupwin32.exe to start the installation program.

3. At the Welcome screen, click **Next**.

4. At the next screen, enter the path location for the Siebel Servers installation, click **Next**.

   For example, C:\seaxx\siebsrvr.

5. The next screen displays the location of the Uninstall program, click **Next**.

6. On the next screen that prompts: **Please stop all Siebel Services before applying the patch**, ensure that the Siebel Service is not running, and click **OK**.

7. The next screen displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

1. Creates a backup folder and moves the existing server files to that folder.

2. Copies the new server file to the proper folder.

3. Installs the Uninstall program.

4. Displays the results of the installation:

If installation is successful, the system displays:	If installation is unsuccessful, the system displays:
Installation was successful. No errors or warnings were generated. Complete log messages are available at: C:\Seaxxx\siebsrv\ICServicePack\7.3.4\SiebelSide\L	ALERT! Installation failed. Please fix these errors and re-run the installer. The following errors or warnings were generated. Complete log messages are available at:

og\install.log	C:\Seaxxx\siebsrv\ICServicePack\7.3.4\SiebelSide\Log\install.log LIST OF ERRORS AND WARNINGS

5. Click **Finish**.

6. If the installation is unsuccessful, run the Uninstall program. Correct the errors and re-run the Installation program.

Siebel Integration component on IC servers

Perform the following steps on the Windows computers that are running IC servers:

1. Go to the folder where you extracted the contents of the ICSide734win.zip file.

2. Open the ICSide734win folder and double-click on setupwin32.exe to start the installation program.

3. At the Welcome screen, click **Next**.

4. The next screen the location of the Uninstall program, click **Next**.

5. The next screen that prompts: **Please stop all IC Services before applying the patch**, ensure that all IC Services are stopped, and click **OK**.

6. The next screen displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

1. Creates a backup folder and moves the existing server files to that folder.

2. Copies the new server file to the proper folder.

3. Installs the Uninstall program.

4. Displays the results of the installation:

If installation is successful, the system displays:	If installation is unsuccessful, the system displays:
Installation was successful. No errors or warnings were generated. Complete log messages are available at: ...\IC73\ICServicePacks\7.3.4\ICSideSiebel\Log\install.log	ALERT! Installation failed. Please fix these errors and re-run the installer. The following errors or warnings were generated. Complete log messages are available at: ...\IC73\ICServicePacks\7.3.4\ICSideSiebel\Log\install.log LIST OF ERRORS AND WARNINGS

5. Click **Finish**.

6. If the installation is unsuccessful, run the Uninstall program. Correct the errors and re-run the Installation program.

Solaris Installation Procedures

The Siebel Integration component must be installed on the computer running Siebel Services and the computer running the IC servers. To have the permissions to run the Solaris installer, you must log in with root privileges.

Siebel Integration component on Siebel server

Perform the following steps on the Solaris computers that are running Siebel Services:

1. At the command line, navigate to the folder where you uncompressed the contents of the SiebelSide734sol.tar file. If the file is compressed, untar the file using the tar -xvpf command.

2. At the command prompt, type `./setupsolarisSparc.bin`.

3. Press **Enter**.

4. On the Welcome screen, click **Next**.

5. At the next screen, enter the path location for the Siebel Servers installation, click **Next**.

   For example, `root/seaxx/siebsrvr`.

6. The next screen displays the location of the Uninstall program, click **Next**.

7. The next screen prompts: **Please stop all Siebel Services before applying the patch**, confirm the Siebel Service is not running and click **OK**.

8. On the next screen that displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

1. Creates a backup folder and moves the existing server files to that folder.

2. Copies the new server file to the proper folder.

3. Installs the Uninstall program.

4. Displays the results of the installation.

If installation is successful, the system displays:	If installation is unsuccessful, the system displays:
Installation was successful. No errors or warnings were generated. Complete log messages are available at: root/Seaxxx/siebsrv/ICServicePack/7.3.4/SiebelSide/Log/install.log	ALERT! Installation failed. Please fix these errors and re-run the installer. The following errors or warnings were generated. Complete log messages are available at: root/Seaxxx/siebsrv/ICServicePack/7.3.4/SiebelSide/Log/install.log LIST OF ERRORS AND WARNINGS

5. Click **Finish**.

6. If the installation was unsuccessful, run the [Uninstall program](#). Correct the errors and re-run the Installation program.

Siebel Integration component on IC server

Perform the following steps on the Solaris computers that are running the IC servers:

1. At the command line, navigate to the folder where you uncompressed the contents of the `ICSide734sol.tar` file.

2. At the command line, type `./setupsolarisSparc.bin`.

3. Press **Enter**.

4. On the Welcome screen, click **Next**.

5. On the next screen, enter the path location for the IC Servers installation and click **Next**.

   For example, `root/IC73`.

6. On the next screen displays the location of the Uninstall program, click **Next**.

7. On the next screen that prompts: **Please stop all IC Services before applying the patch**, ensure that the IC Services are not running, and click **OK**.

8. On the next screen that displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

1. Creates a backup folder and moves the existing server files to that folder.

2. Copies the new server file to the proper folder.

3. Installs the Uninstall program.

4. Displays the results of the installation.

If installation is successful, the system displays:	If installation is unsuccessful, the system displays:
Installation was successful. No errors or warnings were generated. Complete log messages are available at: .../IC73/ICServicePacks/7.3.4ICSideSiebel/Log/install.log	ALERT! Installation failed. Please fix these errors and re-run the installer. The following errors or warnings were generated. Complete log messages are available at: .../IC73/ICServicePacks/7.3.4/ICSideSiebel/Log/install.log LIST OF ERRORS AND WARNINGS

5. Click **Finish**.

6. If the installation was unsuccessful, run the Uninstall program. Correct the errors and re-run the Installation program.

AIX installation procedures

Note: IBM AIX is only supported on Interaction Center Release 7.3, 7.3.1, and 7.3.2. For more information see the Supported Server Operating Systems section in the *Avaya IC Installation Planning and Prerequisites Guide.*

The Siebel Integration component must be installed on the machine running Siebel Services and the machine running IC servers.

Note: To have the permissions to run the AIX installer, you must login with root privileges.

Siebel Integration component on Siebel server

Perform the following steps on the AIX machines that are running Siebel Services.

a. At the command line, navigate to the directory where you uncompressed the contents of the SiebelSide734aix.tar file.

b. At the command prompt, type: `./setupaix.bin`

c. Press **Enter**.

d. On the Welcome screen, click **Next**.

e. On the next screen, enter the location for the Siebel Servers installation, click Next.

For example, root/seaxx/siebsrvr

f. The next screen displays the location of the Uninstall program, click **Next**.

g. On the next screen that prompts, Please stop all Siebel Services before applying the patch, confirm the Siebel Service is not running and click **OK**.

h. On the next screen that displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

- Creates a backup directory and moves the existing server files to that directory.

- Copies the new server file to the proper directory.

- Installs the Uninstall program.

- Displays the results of the installation.

If installation is successful, the system displays:	If installation is unsuccessful, the system displays:
Installation was successful. No errors or warnings were generated. Complete log messages are available at: root/Seaxxx/siebsrv/ICServicePack/7.3.4/SiebelSide/Log/install.log	ALERT! Installation failed. Please fix these errors and re-run the installer. The following errors or warnings were generated. Complete log messages are available at: root/Seaxxx/siebsrv/ICServicePack/7.3.4/SiebelSide/Log/install.log LIST OF ERRORS AND WARNINGS

  i.   Click **Finish**.

  j.   If the installation is unsuccessful, run the [Uninstall program](#). Correct the errors and re-run the Installation program.

Siebel Integration component on IC servers

Perform the following steps on the Solaris machines that are running the IC servers.

  a.   At the command line, navigate to the directory where you uncompressed the contents of the ICSide734aix.tar file. If the file is compressed, untar the file using the tar -xvpf command.

  b.   At the command line, type: **./setupaix.bin**.

  c.   Press **Enter**.

  d.   At the Welcome screen, click **Next**.

  e.   At the next screen, enter the path location for the IC Services installation, and click **Next**.

For example, root/IC73.

  f.   The next screen displays the location of the Uninstall program, click **Next**.

  g.   At the next screen that prompts, Please stop all IC Services before applying the patch, ensure that the IC Services are not running, and click **OK**.

  h.   On the next screen that displays the installation summary, click **Next** to run the installation.

The Installation Tool:

- Creates a backup directory and moves the existing server files to that directory.

- Copies the new server file to the proper directory.

- Installs the Uninstall program.

- Displays the results of the installation.

If installation is successful, the system displays:	If installation is unsuccessful, the system displays:
Installation was successful. No errors or warnings were generated. Complete log messages are available at: .../IC73/ICServicePacks/7.3.2/ICSideSiebel/Log/install.log	ALERT! Installation failed. Please fix these errors and re-run the installer. The following errors or warnings were generated. Complete log messages are available at: .../IC73/ICServicePacks/7.3.2/ICSideSiebel/Log/install.log LIST OF ERRORS AND WARNINGS

    i.   Click **Finish**.

If the installation was unsuccessful, run the Uninstall program. Correct the errors and re-run the Installation program.

Linux installation procedures

Refer Siebel Integration guide for detailed installation instructions.

Import the AICD.def file

To import the AICD.def file, perform the following:

1. Start the Siebel Services.

2. Log in, as Siebel Administrator, to the Siebel Thin Client call center application from the web browser.

3. Navigate to the AICD profile for Siebel, click **Site Map** > **Administration - Communications** > **All configurations**.

4. Select the existing configuration for AICD.

5. Click **Import Configuration**, located on the right side of the window on the **Configurations** tab.

6. A new browser window opens with following text message:

   Caution: Importing communications configuration parameters, commands, events, or drivers and profiles will overwrite all existing definitions of those types in the selected configuration. Click **Next** to proceed.

7. Click **Next**.

8. Select the **Commands** check box.

9. Browse to the AICD.def file.

10. Click **OK**.

Avaya Agent Web Client Connector installation

This section describes the installation procedures for the Avaya Agent Web Client Connector component of the Avaya IC 7.3.4 release. Install the Avaya Agent Web Client Connector on the computer that hosts the Tomcat Server.

- Installation path procedures

- Windows installation procedures

Installation path procedures

The IC 7.3.4 installer checks for the installation path through an environment variable or the registry. The Avaya Agent Web Client Connector installation path is not stored in an environment variable or in the registry. Before starting the Avaya Agent Web Client Connector setup, you must declare the environment variable for the installer to use.

Windows

To declare the Avaya Agent Web Client Connector installation environment variable on Windows, perform the following:

1. Right-click **My Computer**, and select **Properties**.

2. Click the **Advanced** tab.

3. Click **Environment Variables**.

4. In the System variables section, click **New**.

5. In the **New System Variable** dialog box, enter the installation path name and value.

Field Name	Enter
Variable Name	AVAYA_IC73_HOME
Variable Value	The actual installation path, for example: \AvayaWebClientConnector\IC73.

6. Click **OK** to save the new variable.

7. On the **Environment Variables** dialog box, click **OK**.

8. On the **Advanced** tab, click **OK**.

9. Run the Avaya Agent Web Client Connector installation procedures described in Windows installation procedures.

Solaris

To declare the Avaya Agent Web Client Connector installation environment variable on Solaris, perform the following:

1. At the console, type `export AVAYA_IC73_HOME=<Avaya Agent Web Client Connector installation path>`.

   For example, `export AVAYA_IC73_HOME=/opt/AvayaWebClientConnector/IC73`.

2. Press **Enter**.

3. Perform the Avaya Agent Web Client Connector installation procedures as in the following section.

Windows installation procedures

Perform the following steps on the Windows computers that are running the Avaya Agent Web Client:

1. Before you begin the Service Pack Installation, ensure that you have stopped all IC components as explained in Stop Avaya Agent Web Client.

2. Go to the folder where you extracted the contents of the `IC734WinWebConnector.zip` file.

3. Open the IC734WinWebConnector folder and double-click on setupwin32.exe to start the installation program.

4. On the Welcome screen, click **Next**.

5. The next screen displays the location of the Uninstall program, click **Next**.

6. The next screen displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

1. Creates a backup folder and moves the existing web client connector files to that folder.

2. Copies the web client connector files to the proper folders.

3. Copies the files from the Java folder to the proper folders.

4. Installs the Uninstall program.

If installation is successful, the system displays:	If installation is unsuccessful, the system displays:
Installation was successful. No errors or warnings were generated. Complete log messages are available at: ...\IC73\ICServicePacks\7.3.4\WebConnector\Log\install.log	ALERT! Installation failed. Please fix these errors and re-run the installer. The following errors or warnings were generated. Complete log messages are available at: ...\IC73\ICServicePacks\7.3.4\WebConnector\Log\install.log LIST OF ERRORS AND WARNINGS

5. Click **Finish**.

6. If the installation is unsuccessful, run the Uninstall program. Correct the errors and rerun the Installation program.

Solaris installation procedures

To have the permissions to run the Solaris installer, you must log in with root privileges.

Perform the following steps on the Solaris computers that are running the Avaya Agent Web Client:

1. Before you begin the Service Pack Installation, ensure that you have stopped all IC components as explained in Stop Avaya Agent Web Client.

2. Go to the folder where you uncompressed the contents of the `IC734SolWebConnector.tar` file.

3. At the command prompt, type: `./setupsolarisSparc.bin`.

4. Press **Enter**.

5. At the Welcome screen, click **Next**.

6. On the next screen, which displays the location of the Uninstall program, click **Next**.

7. The next screen displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

1. Creates a backup folder and moves the existing web client connector files to that folder.

2. Copies the new web client connector files to the proper folders.

3. Copies the files from the Java folder to the proper folders.

4. Installs the Uninstall program.

5. Displays the results of the installation.

If installation is successful, the system displays: Installation was successful. No errors or warnings were generated. Complete log messages are available at: .../IC73/ICServicePacks/7.3.4/WebConnector/Log/install.log	If installation is unsuccessful, the system displays: ALERT! Installation failed. Please fix these errors and re-run the installer. The following errors or warnings were generated. Complete log messages are available at: .../IC73/ICServicePacks/7.3.4/WebConnector/Log/install.log LIST OF ERRORS AND WARNINGS

6. Click **Finish**.

7. If the installation is unsuccessful, run the Uninstall program. Correct the errors and rerun the Installation program.

Avaya Agent Web Client installation

This section describes the installation procedures for the Avaya Agent Web Client component of the Avaya IC 7.3.4 release.

You must install this component on the computer where the Avaya Agent Web Client package is and not the deployment computer.

This section includes the following topics:

- Installation path procedures

- Windows installation procedures

Installation path procedures

The IC 7.3.4 installer checks for the installation path through an environment variable or the registry. The Avaya Agent Web Client installation path is not stored in an environment variable or in the registry. Before starting the Avaya Agent Web Client setup, you must declare the environment variable for the installer to use.

Windows

To declare the Avaya Agent Web Client installation environment variable on the Windows platform, perform the following:

1. Right-click **My Computer**, and select **Properties**.

2. Click the **Advanced** tab.

3. Click **Environment Variables**.

4. In the System variables section, click **New**.

5. On the **New System Variable** dialog, enter the installation path name and value.

Field Name	Enter
Variable Name	AVAYA_WEBCLIENT73_HOME
Variable Value	The actual installation path, for example: C:\AvayaWebClient\IC73.

6. Click **OK** to save the new variable.

7. At the **Environment Variables** dialog box, click **OK**.

8. On the **Advanced** tab, click **OK**.

9. Run the Avaya Agent Web Client installation procedures described in Windows installation procedures.

Windows installation procedures

Perform the following steps on the Windows computers that are running the Avaya Agent Web Client:

1. Go to the folder where you extracted the contents of the IC734WinWebClient.zip file.

2. Open the IC734WinWebClient folder and double-click on setupwin32.exe to start the installation program.

3. At the Welcome screen, click **Next**.

4. The next screen displays the location of the Uninstall program, click **Next**.

5. The next screen displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

1. Creates a backup folder and moves the existing web client files to that folder.

2. Copies the web client files to the proper folders.

3. Installs the Uninstall program.

4. Displays the results of the installation.

If installation is successful, the system displays: Installation was successful. No errors or warnings were generated. Complete log messages are available at: ...\IC73\ICServicePacks\7.3.4\WebClient\Log\install.log	If installation is unsuccessful, the system displays: ALERT! Installation failed. Please fix these errors and re-run the installer. The following errors or warnings were generated. Complete log messages are available at: ...\IC73\ICServicePacks\7.3.4\WebClient\Log\install.log LIST OF ERRORS AND WARNINGS

5. Click **Finish**.

6. If the installation is unsuccessful, run the Uninstall program. Correct the errors and rerun the Installation program.

7. After successful installation, manually merge the customization files, if any.

8. Generate the war file and deploy on to the webconnector computers.

Note: To generate `webclient.war` file and deploy on Windows Webconnector computers, please see IC7.3 Installation and Configuration guide in Avaya Support Site http://support.avaya.com

Administration and Design installation

This section describes the installation procedures for the IC 7.3.4 Administration and Design component. Only the Windows platform supports the IC 7.3.4 Administration and Design component.

Windows installation procedures

Perform the following steps on each computer where administration tools are installed:

1. Stop the IC Manager, Avaya Database Designer, and the Workflow Designer applications.

2. Go to the folder on the central server where you extracted the contents of the
   `IC734WinAdmin.zip` file.

3. Copy the IC734WinAdmin folder to the computer where you want to install the Admin
   component. If you are accessing a network computer through a mapped drive, do not copy the
   folder. Perform the following steps from your administration computer:

   a. Open the IC734WinAdmin folder on the computer from which you want to install.

   b. Double-click the setupwin32.exe to start the installation.

   c. On the Welcome screen, click **Next**.

   d. The next screen displays the location of the Uninstall program, click **Next**.

   e. In the pop-up window that prompts: **Please log out from IC Manager**, click **Continue**.

   f. The next screen displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

1. Creates a backup folder and moves the existing admin files to that folder.

2. Copies the new admin files to the proper folders.

3. Registers the new .ocx and .dll files.

4. Installs the Uninstall program.

5. Displays the results of the installation.

If installation is successful, the system displays:	If installation is unsuccessful, the system displays:
Installation was successful. No errors or warnings were generated. Complete log messages are available at: ...\IC73\ICServicePacks\7.3.4\DesignAdmin\Log\install.log	ALERT! Installation failed. Please fix these errors and re-run the installer. The following errors or warnings were generated. Complete log messages are available at: ...\IC73\ICServicePacks\7.3.4\DesignAdmin\Log\install.log LIST OF ERRORS AND WARNINGS

6. Click **Finish**.

7. If the installation is unsuccessful, run the Uninstall program. Correct the errors and re-run the
   Installation program.

Avaya Agent (rich client) installation

This section describes the installation procedures for the IC 7.3.4 Avaya Agent (rich client) component. Only
the Windows operating system supports the Avaya Agent installation.

Note: You can install the IC 7.3.4 Avaya Agent (rich client) component after you have installed and configured all other IC 7.3.4 SP components. You do not require stopping the IC Servers before installing the IC 7.3.4 Avaya Agent (rich client) component.

Installation procedures

Perform the following steps on each agent workstation:

1. Stop the Avaya Agent application if it is running.

2. Go to the folder on the computer where you extracted the contents of the `IC734WinAgentClient.zip` file.

3. Copy the IC734WinAgentClient folder to the computer where you want to install the Agent component. If you are accessing a network computer through a mapped drive, do not copy the folder. Perform the following steps from your agent desktop computer:

   a. Open the IC734WinAgentClient folder and double-click on setupwin32.exe to start the installation program.

   b. In the Welcome window, click **Next**.

   c. The installation runs the Preinstall options that unregister the .ocx and .dll files that are patched in this installation.

   d. The next screen displays the location of the Uninstall program, click **Next**.

   e. In the pop-up window that prompts: **Please logout Avaya Agent**, click **Continue**.

   f. The next screen displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

1. Creates a backup folder and moves the existing agent files to that folder.

2. Copies the new agent files to the proper folders.

3. Registers the new .ocx and .dll files.

4. Installs the Uninstall program.

5. Displays the results of the installation.

If installation is successful, the system displays: Installation was successful. No errors or warnings were generated. Complete log messages are available at: ...\IC73\ICServicePacks\7.3.4\AvayaAgent\Log\install.log	If installation is unsuccessful, the system displays: ALERT! Installation failed. Please fix these errors and re-run the installer. The following errors or warnings were generated. Complete log messages are available at: ...\IC73\ICServicePacks\7.3.4\AvayaAgent\Log\install.log LIST OF ERRORS AND WARNINGS

6. Click **Finish**.

7. If the installation is unsuccessful, run the <u>Uninstall program</u>. Correct the errors and re-run the Installation program.

8. If the installation is successful, reboot the agent computer.

Avaya Agent installation in silent mode

On the Windows platform, you can also run the IC 7.3.4 Avaya Agent installation in silent mode. The silent mode option is for Avaya Agent installations on multiple computers.

To run the installer in silent mode, run record mode followed by silent mode.

- In record mode, the installer runs the installation normally but records all of your inputs in a text file.

- In silent mode, rerun the same installation in silent mode on another computer using the inputs from this text file.

Record mode

To run the installer in record mode, perform the following:

1. Click **Start** > **Programs** > **Accessories** > **Command Prompt**.

2. Go to the package folder where the contents of the FP installer are extracted.

3. At the command prompt, type：

   `setupwin32.exe -options-record <AbsolutePathOfFile.ext>.`

Note: The `<AbsolutePathOfFile.ext>` is a placeholder for the qualified complete file name, where `AbsolutePathOfFile` is the name of the file and `ext` is the file extension.

4. Press **Enter**.

5. Complete the installation using the information in Avaya Agent (rich client) installation. The installer creates the `<AbsolutePathOfFile.ext>` file containing all of your inputs.

Silent mode

To rerun the installer in silent mode, perform the following:

1. Copy the `<AbsolutePathOfFile.ext>` file to the computer where you want to install.

2. Click **Start** > **Programs** > **Accessories** > **Command Prompt**.

3. Go to the package folder where the contents of the FP installer are extracted.

4. At the command prompt, type:

   `setupwin32.exe -options <AbsolutePathOfFile.ext> -silent`

   For example: `setupwin32.exe -options "D:\temp\SPSilent.opt" -silent`

5. Press **Enter**.

   The installation runs (without a GUI) using the **<AbsolutePathOfFile.ext>** file for your inputs.

Comments on this document? infodev@avaya.com

Chapter 4: IC 7.3.4 Configuration

Before you apply configurations, you need to start Core IC Servers as mentioned below.

Start Core IC servers

To start the ORB server on the server computer:

1. At the command prompt, navigate to the following folder:

   - Windows: `...\IC73\bin`.

   - Solaris, AIX and Linux: `.../IC73/bin`.

2. Type the following command:

   - Windows: `icadmin so`.

   - Solaris, AIX and Linux: `./icadmin so`.

3. Press **Enter**.

Mandatory Configurations

Following configurations are mandatory to perform so that IC 7.3.4 SP functions properly.

Merging and importing the sc.xml file

Merging
If you have performed any customization in the existing `sc.xml` file, you must merge those changes from the backed up file (See above "sc.xml" section). Backup the `<AVAYA_IC73_HOME>\etc\sc.xml` file and merge you changes. Then copy the merged `sc.xml` at the same location `<AVAYA_IC73_HOME>\etc`.

Note:

- If you have merged any previous customization changes in the new `sc.xml` file, check the xml syntax is proper.

Importing
To import the `sc.xml` file, perform the following:

1. Log on to IC Manager as Admin.

2. From the IC Manager, click **Manager** > **Options** > **Environment** tab.

3. Click **Import Configuration**.

4. From the **Open** dialog box, select the `sc.xml` file that you copied in step 2, and click **Open**.

5. If the file is successfully validated, the **Validate sc.xml** dialog box displays a Successfully Validated message. If the validation is unsuccessful, the system displays an xml parsing error.

6. Logout and login into IC Manager

Merging and Pushing the AARC Scripts

Merging

If you have performed any customization in the existing AARC scripts, you must merge those changes from the backed up file (See above "AARC scripts" section).

For example: If there is change in `CoreServices_Login.qsc` then merge the changes in `Avaya_IC73_HOME\design\QConsole\CoreServices_Login.qsc` file.

Importing

1. Start the Avaya Database Designer.

2. Push the scripts to the database using Generate Windows Application.

Java/Tomcat Configuration

In IC 7.3.4 SP, Java and Tomcat are upgraded. Therefore all Avaya IC services need to be deleted and re-deployed using config tool.

Steps to be performed the machine where the specific services are deployed:

1. Stop all the IC services including following
    a. Avaya IC Email Template Management Service 7.3
    b. Avaya IC ICM Service 7.3
    c. Avaya SDK Services 7.3
    d. Avaya IC Test 7.3
    e. Avaya IC Web Management Service 7.3
    f. Avaya IC WebLM Service 7.3
    g. Avaya IC CIRS Service 7.3

       h.   Avaya IC CSPortal Web Service 7.3

2. Run Config tool and uncheck following options

       a.   Configure Web License Manager

       b.   Configure Email Template Administration

       c.   Configure Web Management

       d.   ICM

       e.   IC Test

3. Apply the changes.

4. Restart the machine.

     Note: After machine restarted, you need to start IC Core Servers. Refer Start Core IC Servers above to start servers.

5. Clean the tomcat cache by deleting the content of following directory: <Avaya_IC73_Home>\tomcat\work\Catalina\localhost\

6. Launch Config-tool.

7. Select all the services de-selected in #2 above.

     Note: When you select "Configure Email Template Administration", you need to provide "**Email Template Administrator Login**" and "**Email Template Administrator Password**". For example Login user as "dcobridge1" and Password as "dcobridge1".

8. Click "Apply Settings".

9. Perform following WebLM configurations

       a.   Stop the Tomcat server

       b.   Restore/Overwrite the set of files you have backed up (see above "WebLM Files" sub-section in Backup Configuration Files section) in the respective file/folder location.

       c.   Locate the `server.weblm.xml` file. It is normally located under the `<AVAYA_IC73_HOME>/tomcat/conf` folder.

       d.   Go to end of file and add Connector tag for port 52233 which will be used as the HTTPS port for WebLM. The following element should be added before the element `</Service>`

Note: As per the Licensing Conformance Requirements [125163-M-850], licensed products shall utilize port 52233 for HTTPS communication with WebLM server.

Configuration for Tomcat Installation without APR **:

```
<Connector acceptCount="100" clientAuth="false"
disableUploadTimeout="true" enableLookups="false"
keystoreFile="${catalina.base}/webapps/WebLM/WEB-INF/weblmserver.p12"
keystorePass="password" SSLEnabled="true" keystoreType="PKCS12"
maxHttpHeaderSize="8192" maxSpareThreads="75" maxThreads="150"
minSpareThreads="25" port="52233" scheme="https" secure="true"
sslProtocol="TLS"
ciphers="SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA,SSL_DH_RSA_WITH_3DES_EDE_CBC_
SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA,TLS_K
RB5_WITH_3DES_EDE_CBC_MD5,TLS_KRB5_WITH_3DES_EDE_CBC_SHA,TLS_ECDH_ECDSA
```

```
_WITH_3DES_EDE_CBC_SHA,TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_ECD
SA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_DS
S_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WIT
H_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128
_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128_CBC_S
HA,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128_CBC_SH
A,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SH
A,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_S
HA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA"/>
```

Configuration for Tomcat Installation with APR**:

```
<Connector acceptCount="100" clientAuth="false"
disableUploadTimeout="true" enableLookups="false"
SSLPassword="password" SSLEnabled="true" maxHttpHeaderSize="8192"
maxSpareThreads="75" maxThreads="150" minSpareThreads="25" port="52233"
scheme="https" secure="true" sslProtocol="TLS"
SSLCipherSuite="ALL:!ADH!RC4 -IDEA:!LOW:!SSLv2:!EXPORT40!EXPORT56"
SSLCertificateFile="${catalina.base}/webapps/WebLM/WEB-INF/weblm.crt"
SSLCertificateKeyFile="${catalina.base}/webapps/WebLM/WEB-
INF/weblm.key"/>
```

Note: This is assuming that WebLM is deployed in `<tomcat_installation_dir>/webapps` folder. Be careful while doing a copy paste from this document into the `server.xml` file. Ensure that the valid quotes are copy pasted in the `server.xml` file.

    e. For the Connectors on port 8080 and 8009, update the value of attribute `redirectPort` from (default) 8443 to 52233.

    f. Start Tomcat/WebLM service and access WebLM.

    g. In the Web browser, enter the URL of the WebLM server in the following format:

       https://<IP_Address>:52233/WebLM/index.jsp

Steps to be performed on WebConnector machine:

1. Execute `< AVAYA_IC73_HOME >\bin\aawcclient.bat stop`

2. Remove the `aawcclient.bat` from `<Avaya_IC73_Home>\bin`

3. Run config tool.

4. Go to "Web Client" tab and click on Apply.

5. To create new war file, execute `<AVAYA_IC73_HOME>\bin\aawcclient.bat start`

6. Redeploy the newly created `webclient.war` file. For more information, see IC 7.3 Installation and Configuration guide.

Database Configuration

The database can be reconfigured with the following steps:

1. Merge existing customizations in ADL. If you are upgrading from 7.3.3 FP you can skip this step.
2. Add new Enums and Reconfigure the database.
3. Import new properties. If you are upgrading from IC 7.3.2 or IC 7.3.3 FP you can skip this step.

Merge existing customizations in ADL

IC 7.3.4 service pack contains `ccq_733.adl` and `repository_733.adl` file in
`<AVAYA_IC73_HOME>`/design/CallCenterQ and `<AVAYA_IC73_HOME>`/design/repository folders
respectively. You must manually merge your customizations with `ccq_733.adl` and `repository_733.adl`
before performing database administration.

Add new Enums and Reconfigure the database

1. Log on to the IC73 Design and Admin computer.

2. Launch the Database Designer application.

3. Using **File** > **Open** menu option, select the file:
   `<AVAYA_IC73_HOME>\design\repository\repository.adl`.

4. Open `classificationcode` table

5. Add the following enums for Database Field "`codetype`" in table "`classificationcode`" as
   shown below:

   - `"7-Wrapup Code Type"`

   - `"8-Wrapup Code Value"`
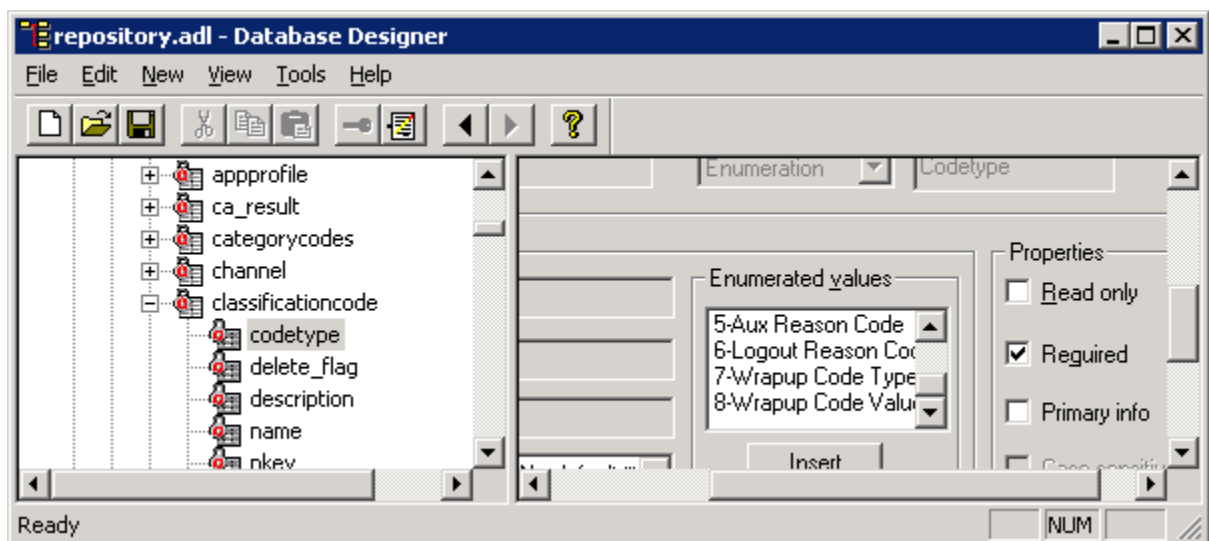
6. Reconfigure the database and Generate Windows Application using the normal reconfiguration procedure. For more information, see Admin guide.

7. Close the ADL file using **File** > **Close** menu option.

8. Using **File** > **Open** menu option, select the file:
   `<AVAYA_IC73_HOME>\design\CallCenterQ\ccq.adl`.

9. Repeat steps 4 to 7 for ccq.adl.

Import new properties (TemplateDownload and StatusDownload - Introduced in IC 7.3.2 SP)

Note: If you are upgrading from IC 7.3 RTM or IC 7.3.1 SP, only then perform following steps:

1. Log on to the IC 7.3.4 Design and Admin computer.

2. Go to command prompt.

3. Change folder to repository data `<AVAYA_IC73_HOME>/design/repository/data`.

4. Execute the `import_properties.bat` command by passing arguments `<Admin_Name>` & `<Admin_Password>`

5. For more details about success or failure please check the `<AVAYA_IC73_HOME>\logs\General_Admin.log` file.

Import the seed data (Introduced in IC 7.3.3 FP)

Note: If you are upgrading from IC 7.3.3 FP, then this step is not required.

To import the new seed data introduced in 7.3.3, perform the following:

1. Open a command prompt and enter `<IC_HOME>\design\CallCenterQ\delta`.

2. Open `migrate_seed.cfg` in an ASCII editor, Notepad, and verify the administration login ID and password are correct.

3. Add following statement to the # tables section:

   ```
   Table=w_qw_prop_class,w_qw_prop_class_733_delta
   Table=w_chat_prop_inst,w_chat_prop_inst_733_delta
   ```

4. For localization support you add following statement to the # tables section already mentioned and also as follows:

   ```
   Table=w_chat_prop_inst,w_chat_prop_inst_L10N_733_delta
   ```

5. Comment other #Table entries.

6. Save and close the `migrate_seed.cfg` file.

7. Run `migrate_seed.bat` or on command prompt run following command:

```
..\..\..\bin\qimport import migrate_seed.cfg
```

HTTPS Configuration

If you have configured HTTPS, restore the backed up files (See above "Certificate Files" sub-section in Backup configuration Files section).

Copy backed up certificate and keystore files in `AVAYA_IC73_HOME\Java\lib\security` folder.

Exchange 2010 configuration changes

Required settings for the account configured on Microsoft Exchange server, when used by the website to send the email.

Website fails to send an email into the IC system if it uses an email account configured in the IC Manager with SMPT authentication enabled (outgoing email server tab). To make this work the Exchange server requires additional permission for the receive connector used by the website.

Steps to give additional permission to the account:

1. Identify the email account used by website for sending the email into the IC system which is configured in IC Manager.

Note: You can identify the email account by looking into the website logs, `website_debug.log` with full debug enabled.

   a. Send an email from the website.

   b. Search for the below log snippet:

      – EmailEscalate: sendEmail:: Able to get the email account for the emailaddress [@support@ccms.apac.avaya.com :]

      – Where: support@ccms.apac.avaya.com is <Name>@<Domain> of email account configured in the IC Manager

   c. Look for the configured email account <Name> in the IC Manager. This account is used by the website to send the email into the IC system.

2. After identifying the account, Exchange server requires to set additional permission on the receive connector uses by the website:

   a. Run the Microsoft Exchange command shell.

   b. To set the permission on the receive connector run the below commands for the IC account:

      – `Get-ReceiveConnector "<Machine_Name>\<Receive_Connector_Name>" | Add-ADPermission -User "<Domain_Name>\<userLogon_Name>" -ExtendedRights "Ms-Exch-SMTP-Accept-Any-Sender"`

- Get-ReceiveConnector "<Machine_Name>\<Receive_Connector_Name>" | Add-ADPermission -User "<Domain_Name>\<userLogon_Name>" -ExtendedRights "Ms-Exch-SMTP-Accept-Authoritative-Domain-Sender"

For example:

`SANCCMS1.ccms.lab.com` = FQDN name for the computer hosting the exchange server.

customer@ccms.lab.com = User Account configured on the exchange used by the IC website to send the email.

Default SANCCMS1 = Receive connector used by the IC website.

```
Get-ReceiveConnector "SANCCMS1\Default SANCCMS1" | Add-ADPermission -User
"ccms\customer" -ExtendedRights "Ms-Exch-SMTP-Accept-Any-Sender"
```

```
Get-ReceiveConnector "SANCCMS1\Default SANCCMS1" | Add-ADPermission -User
"ccms\customer" -ExtendedRights "Ms-Exch-SMTP-Accept-Authoritative-Domain-
Sender"
```

Note: These permissions are specific to the Receive connector used by the website, so before running the command ensure that you use the right Receive connector. For example, if there is Receive connector created other than default to receive the email from the website then you must specify that particular Receive connector in the command. To identify the Receive connector check the smtpreceive logs after enabling the verbose logging. Location for the log is:

```
<Microsoft_Exchange Server_HOME>\V14\TransportRoles\Logs\ProtocolLog\SmtpReceive
```

Send an email from the website and check the received connector name handling the email send by the website (IP of the computer hosting the website).

c. Restart the Microsoft Exchange Transport service.

d. Make sure the Receive connector has checkbox enabled for **Anonymous users** under the **Permission Group** tab.
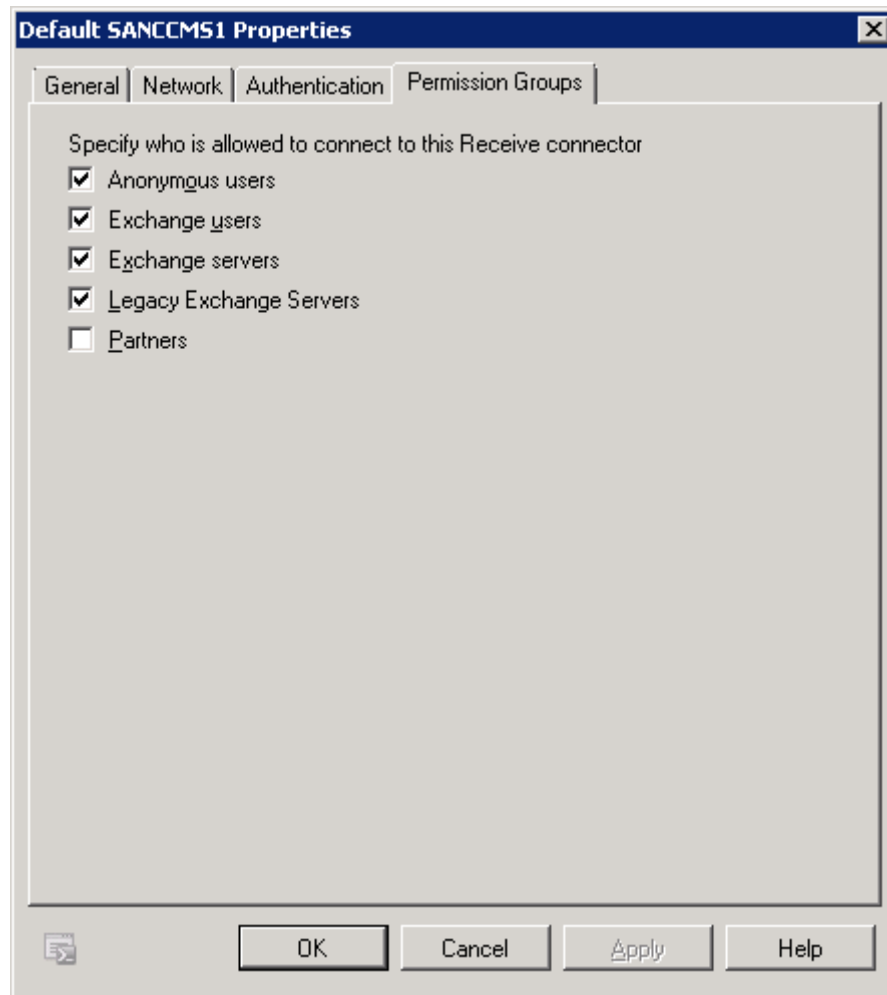
Exchange 2013 configuration changes

Exchange server 2013 is more restrictive in terms of the relaying the email, additional privileges must be given to the user account used by the website.

1. Run the commands mentioned above (2013 exchange) in the Exchange server command shell.

2. Search for the user account, the account created in the exchange for IC, in the Active folder.

3. Right-click and open the properties of the account.

4. Assign the user as a member of **Organization Management** group from tab **Member of**.

5. Ensure after performing these changes the exchange services are restarted such as:

   ▪ Microsoft Exchange Frontend Transport

   ▪ Microsoft Exchange Mailbox Transport Delivery

IIS-Tomcat Redirector configuration (Introduced in IC 7.3.2 FP)

If you are upgrading from IC 7.3.2 FP or higher FP/SP, then this configuration is not required.

When you host a customer website on Internet Information Services (IIS), a third-party ISAPI filter is used to redirect requests for the IC website to the Tomcat server that hosts the Web Management Service. This filter, `isapi_redirect.dll`, is also known as Tomcat Redirector. The Tomcat Redirector has been upgraded in IC 7.3.2 FP.

IC ships Tomcat Redirector with the RTM installer for customers to use the filter, if required. When you deploy the IC website, the configuration tool installs the ISAPI filter to be used with IIS on Windows.

For the Tomcat Redirector to function properly, certain configurations are required on the IIS side:

The application pool, under which the website runs, must have worker recycling disabled.

1. To determine the application pool under which the website runs, click the website, and select **Advanced Settings** in the **Actions** panel. The **Application Pool** used for the website can be read or set from the dialog box that the system displays. Make note of the application pool.

2. Click the **Application Pool Node**. Select the application pool noted in the previous step, and click **Advanced Settings** from the **Action** panel.

3. Make the following changes to the settings:

   a. Set Limit Interval under CPU to 0.

   b. Set Idle Time-out under Process Model to 0.

   c. Set Regular Time Interval under Recycling to 0.

   d. Set Disable Recycling for configuration changes under Recycling to true.

Typically, the Tomcat Redirector is installed on a customer facing website, and the Tomcat server resides in the local LAN across a firewall. Problems can occur with idle connections due to firewalls that are often deployed between the web server layer and the backend. Depending on the configuration, the firewall can silently drop connections from the status table after the configuration. The Tomcat Redirector and the Tomcat server treat this situation as when the other side is not answering any traffic.

However, since TCP is a reliable protocol, it detects the missing TCP ACKs and tries to resend the packets for a relatively long time, typically several minutes. Therefore, the Tomcat Redirector or Tomcat server is not able to detect connection loss until after some time.

Firewall related configurations are provided to minimize issues due to connection drops due to firewall timeouts:

1. You must always use `connection_pool_timeout` and `connection_pool_minsize` on the Tomcat Redirector side and `connectionTimeout` on the Tomcat side to prevent idle connection drop.

---

2. The recommended value for the `connection_pool_timeout` parameter is approximately 10 minutes. Therefore, set the value for the `connection_pool_timeout` parameter to 600 seconds. If you use this attribute, also set the attribute `connectionTimeout` in the AJP Connector element of your Tomcat website.server.xml configuration file to an analogous value.

Note: The `connectionTimeout` parameter is in milliseconds. Therefore, if you set Tomcat Redirector `connection_pool_timeout` to 600, you can set the Tomcat `connectionTimeout` parameter to 600000.

The Tomcat Redirector is upgraded in this service pack and consequently some of the directives used in the Tomcat Redirector configuration files have changed. For more information, see http://tomcat.apache.org/connectors-doc/reference/workers.html.

Using Lower case for Agent ID in custom SDK clients (Introduced in IC 7.3.1 SP)

From SP 7.3.1 onwards, the SDK server does not convert the Agent ID from the incoming login request to lowercase as it results into unexpected behavior subsequently. The SDK now passes the login request for authentication as it receives. The SDK sample clients are changed to convert the Agent ID from the login request into lower case before sending to SDK Server for authentication.

The custom SDK clients must have logic to convert the Agent ID to lower case before sending the login request to the SDK server.

Disabling SQL Injection filter for Website

The SQL Injection filter in web.xml file of website should be disabled IC 7.3.4 onwards. SQL Injection attack is prevented even without this filter.

This configuration is required if:

- SQL Injection filter has been enabled in web.xml of website. By default the SQL Injection filter is disabled.

Perform these steps on the IC server where you have deployed the website. The following procedure is for the Windows platform. The steps are the same for Solaris and AIX platforms except for the file and folder naming conventions and difference of method of starting and stopping the Tomcat web server.

1. Go to the `%AVAYA_IC73_HOME%\comp\website\WEB-INF` location. Backup the `web.xml` file.

2. Open the `web.xml` file using a Text Editor.

3. Locate the filter by name, `sqlAttackFilter`, shown as `<display-name>sqlAttackFilter</display-name>`.

4. If the filter is already commented with `<!--` symbol, the SQL Injection filter is disabled and you can ignore the below steps. (An example of how a commented filter looks has been shown in step 6)

5. Stop the IC Website. For more information, see the IC Install and Configuration guide.

6. Comment the entire filter and its corresponding filter mapping by adding `<!--`at the beginning of the filter and `-->` at the end of the filter-mapping section of the `sqlAttackFilter`. Here is how it should look:

```
<!-- website sqli start

        <filter>

                <description>This filter is used to detect
SQLI.</description>

                <display-name>sqlAttackFilter</display-name>

                <filter-name>sqlAttackFilter</filter-name>

                …

        </filter>

        <filter-mapping>

                <filter-name>sqlAttackFilter</filter-name>

                <url-pattern>/admin/*</url-pattern>

        </filter-mapping>

    website sqli end -->
```

7. Save and close this file.

Start the IC Website. See the IC Install and Configuration guide for the platform specific start and stop procedure.

Upgrading IC SDK

You must manually replace the IC SDK Server files installed on the Windows, Solaris, and AIX platforms if you have installed and configured the IC SDK Server.

Perform the following configuration steps to replace the files:

1. Extract `icsdk.war` on local computer, for example: `c:\icsdkextract\`.

2. Backup all jar files from the `%AVAYA_IC73_HOME%\sdk\server\icsdk\WEB-INF\lib\` location and manually copy all jar files from above extracted folder, for example: `c:\icsdkextract`, to `%AVAYA_IC73_HOME%\sdk\server\icsdk\WEB-INF\lib\`.

3. Backup following files from `%AVAYA_IC73_HOME%\sdk\design\dotnet\lib` folder and manually copy the following files from sdk folder of IC 7.3.x Service Pack to the `%AVAYA_IC73_HOME%\sdk\design\dotnet\lib folder`:

- ▪ `AvayaICSDKClient.dll`

- ▪ `AvayaICSDKClient.pdb`

- ▪ `AvayaICSDKClient.xml`

- ▪ `Com.Avaya.Util.dll`

- ▪ `Com.Avaya.Util.Messaging.dll`

- ▪ `Com.Avaya.Util.Messaging.pdb`

- ▪ `Com.Avaya.Util.pdb`

- ▪ `CSharptester.pdb`

4. Backup following files from `sdk\design\dotnet\sample\bin` folder and manually copy the
   following files from sdk folder of IC 7.3.x Service Pack to the
   `%AVAYA_IC73_HOME%\sdk\design\dotnet\sample\bin folder`:

- ▪ `AvayaICSDKClient.dll`

- ▪ `AvayaICSDKClient.pdb`

- ▪ `AvayaICSDKClient.xml`

- ▪ `Com.Avaya.Util.dll`

- ▪ `Com.Avaya.Util.Messaging.dll`

- ▪ `Com.Avaya.Util.Messaging.pdb`

- ▪ `Com.Avaya.Util.pdb`

- ▪ `CSharptester.exe`

- ▪ `CSharptester.pdb`

5. Backup the following folders from the specified folder location and manually copy the following
   from the IC 7.3.x Service Pack to the specified folder location:

- ▪ The Controller and UI folders from
   `sdk\design\dotnet\sample\src\Com.Avaya.Ic.Sdk.Sampleclient`.

- ▪ The Doc folder from `sdk\design\java\doc`.

- ▪ The src folder from `sdk\design\java\sample`.

6. Ensure that the newly copied files have the same read/execute permissions as the backed-up
   files.

Start Other IC Servers

In IC Manager, you must start the IC servers individually and in the proper order. To start IC servers in IC Manager perform the following:

1. Click the **Server** tab and select the server to be started.

2. Click **Start Server**.

3. The following table lists the order in which to start the servers:

Server Category	Server Name
Core Engine servers	Alarm server, Data server, Directory server, License server
Reporting Services	Event Collector server, Report server
DU (Data Unit) servers	ADU server, DUStore server, EDU server
Web Management servers	WebACD server, Web Admin Adapter (WAA) server, Attribute server, ComHub server, Paging server, Web Schedule Callback
Email Management servers	ICEmail server (requires the WebACD server), CAServer server, CAAdmin server
Telephony servers	Telephony and TSQS servers (all switches), Telephony Server, Adapter (TSA) server, Predictive Dialing Kernel (Outbound Contact) server, Soft Dialer server, VOX server
Business Logic servers	Workflow server, Blender server, Notification server
Web and Support servers	HTTP Connector server, WebQ server, WebQ Router server
Siebel Native Integration	ASIS Server

Start IC services

After you complete the Avaya IC 7.3.4 Server installation program, you must start all IC Services on all of the machines (if multi-box setup).

Windows

The steps given in this section are for the Windows platform.

To start the IC Services perform the following:

1. Start the Windows Services application.

2. Start any of the following services that are not already started. Some might not exist on every server.

   - Avaya IC CIRS Service 7.3

   - Avaya IC Email Template Management Service 7.3

   - Avaya ICM Service 7.3

   - Avaya IC ORB Service 7.3

   - Avaya IC Test Service 7.3

   - Avaya IC Web Management Service 7.3

   - Avaya IC WebLM Service 7.3

   - Avaya IC CSPortal Web Service 7.3

   - Avaya Voice Media Manager

   - Avaya SDK Services

   - Avaya Business Advocate Component Manager

Solaris

To start the IC Services perform the following:

1. Go to the `.../IC73/bin` folder.

   - For ICM:

     a. At the command prompt, type: `./icm.sh start`.

     b. Press **Enter**.

   - For CIRS:

     a. At the command prompt, type: `./cirs.sh start`.

     b. Press **Enter**.

   - To start multiple Tomcat instances:

     a. At the command prompt, type: `./ictomcat.sh start all`.

     b. Press **Enter**.

- To start single Web application:

    a. At the command prompt, type: `./ictomcat.sh start <servicename>`.

    b. Press **Enter**.

- For the Oracle iPlanet Server:

    a. Start Oracle iPlanet Web server.

    b. Go to `<Oracle-iPlanet-Web-Server_HOME>/admin-server/bin/` path.

    c. Type `./startserv`.

    d. Press **Enter**.

    e. Go to `<Oracle-iPlanet-Web-Server_HOME>/<https-node-name>/bin/` path.

    f. Type command `./startserv`.

    g. Press **Enter**.

Start Avaya Agent Web Client

After you run the IC 7.3.4 installation, you can start the Avaya Agent Web Client component by handling the javaw process.

To start the javaw process, perform the following:

1. Click **Start** > **Run** to open the command prompt.

2. Change the folder to: `AVAYA_IC73_HOME \bin`.

3. Execute the following commands:

Operating System	Procedure
Windows	To start: `aawcclient.bat start`
Solaris	To start: `./aawcclient.sh start`

Configurations to preventing duplicate chat

Majority of the IC customers using the chat channel use the out-of-the-box (OOTB) website core engine to escalate chat into the IC system.

The OOB chat gathers user inputs using the `escalate.jsp` page. Thereafter, the customer is directed to the `htmlcclient.jsp` page where the actual chat begins with an agent. All the requisite parameters required for successful chat escalation are in the form of request parameters appended to the `htmlclcient.jsp` URL.

There is a possibility that a chat might be re-escalated within the IC system in following scenarios:

- Some browsers provide the facility of storing and reopening the last browsed-session pages. Therefore, if the user closes the browser after the chat ends, there is a possibility that the chat might get re-escalated within the IC system unintentionally.

- The user unintentionally refreshes the page after the chat ends.

The expected behavior is that the user must fill in the details and the initial question for every attempt to escalate a live chat to an Agent.

Note: Only Avaya APS or Avaya channel partners must perform the following procedure:

To enable the prevention of redundant chat for the customized chat solution, perform the following steps:

1. Add specific Metadata properties.

2. Set/Unset specific browser cookie attributes.

3. Set specific attributes as part of the Java HttpSession Object.

4. Change the Warning text messages of the redirected URL, if required.

Add the following metadata properties

1. In a Web browser, navigate to the IC Website administration page:

   `http://<server_name>/website/admin/login.jsp`

2. Enter the user name and password. Click **Next** to log in to the IC Website administration page.

3. Access the add metadata page:

   `http:// <server_name>/website/admin/tenancy/addmd.jsp`

4. Add the following metadata properties:

   - Metadata name = `chat.htmlclient.redundant.action.`

   - Default value = none. Change this value to one of the other values as specified in the Description.

   - Description = Determines what action must be taken after redundant chat is detected. Valid values are redirect, alert, custom or none.

Note: The custom value must be used only if Avaya APS or channel partners who deploy the SP provide some other custom solution.

5. Click Add Metadata.

6. Add the following metadata properties:

   - Metadata name = `chat.htmlclient.undocked.sessionexpirepage`.

   - Default value = `htmlclient/chatsessionexpire.jsp`.

   - Description = For undocked chat, determines which page must be shown if the customer tries to escalate a chat by refreshing the undocked chat page, `chatFrame.jsp`.

   - This particular page must be at the following folder location: `%AVAYA_IC73_HOME%\comp\website\public` folder.

7. Close the browser.

Note: Clear off the Tomcat work folder contents of public IC Website application, `%AVAYA_IC73_HOME%\tomcat\work\Catalina\localhost\website\org\apache\jsp\public`, and restart the website.

Setting specific browser cookie attributes

1. The `chat_escalate` cookie is set to true as part of the `escalate.jsp` page. Set this cookie to false when the customer escalates a successful chat for the first time.

2. The `aicEscStartURL` cookie is set to `wru.jsp` and remains set in the browser page of the customer. This URL is the page that the customer sees in the docked window when the chat is escalated.

3. Optional Step: Set the Domain attribute as part of the cookie initialization. The OOTB website has the cookie setting code where the Domain attribute must be set and this is based on the customer configuration of the chat pages.

   - `escalate.jsp`. (`%AVAYA_IC73_HOME%\comp\website\public` folder).

   - `htmlchatrcc.jsp` (`%AVAYA_IC73_HOME%\comp\website\public\htmlclient` folder).

   - `chathandler.js.jsp` (`%AVAYA_IC73_HOME%\comp\website\public\htmlclient` folder).

The first two attributes must be set as part of the browser cookie of the customer. These attributes are set before the customer can escalate a chat.

Setting specific attributes as part of the Java HttpSession Object

1. role: Customer for a authenticated customer or guest otherwise.

2. tenant: The tenant name.

3. sessionUser: Type `com.quintus.usermanager.User`, which further sets the attribute role as one of its Map parameters. For more information, see OOTB account.jsp.

The first two parameters must be part of the HttpSession Object before a successful chat escalation.

Changing the Warning text messages of the redirected URL

This is applicable for `chat.htmlclient.redundant.action` = redirect case only.

- On detecting that a duplicate chat is being escalated, for a docked/undocked chat, the customer is redirected to an `escalate.jsp` page where a warning is shown to the customer.

You can customize this warning message for each customer upon redirection. Look for `warningText` attribute of the `escalate.jsp` page.

OOB Chat Behavior for various chat.htmlclient.redundant.action attributes

The following tables show the OOTB chat behavior for various `chat.htmlclient.redundant.action` attributes:

chat.htmlclient. redundant.action	First valid chat escalation	Successive chat escalation, accessing the htmlclclient.jsp page directly [DOCKED/VALID USER SESSION]	Successive chat escalation, accessing the htmlclclient.jsp page directly [UNDOCKED/VALID USER SESSION]
none	Chat would be escalated.	Allow the chat to be escalated.	Allow the chat to be escalated.
redirect	Chat would be escalated.	User would be redirected to `escalate.jsp` page.	The popup `chatframe.jsp` would be closed and the user would be redirected to `escalate.jsp` page.
alert	Chat would be escalated.	A popup option would be displayed asking the user if he wants to escalate the chat **OK**: Will escalate the chat again. **Cancel**: Will prevent the chat escalation.	A popup option would be displayed asking the user if he needs to escalate the chat. **OK**: Will escalate the chat again. **Cancel**: Will prevent the chat escalation.

chat.htmlclient. redundant.action	Successive chat escalation, accessing the htmlclclient.jsp page directly [UNDOCKED/INVALID USER SESSION]	Successive chat escalation, refreshing the chatframe.jsp page directly [UNDOCKED/VALID USER SESSION]	Successive chat escalation, refreshing the chatframe.jsp page directly [UNDOCKED/INVALID USER SESSION]
none	Closing and opening the browser by waiting for session to expire, the user would be redirected to escalate and hence `account.jsp` page.	Allow the chat to be escalated.	Closing and opening the browser by waiting for session to expire, the user would be redirected to escalate and hence `account.jsp` page.
redirect	Closing and opening the browser by waiting for session to expire, the user would be redirected to escalate and hence `account.jsp` page.	User would be redirected to `chatsessionexpire.jsp` page.	Closing and opening the browser by waiting for session to expire, the user would be redirected to escalate and hence `account.jsp` page.
alert	If the user presses the Ok button after the session expires then the chat escalation would fail eventually. Also accessing the `htmlclient.jsp` page directly after the user session has expired would redirect him to escalate and hence `account.jsp`.	A popup option would be displayed asking the user if he needs to escalate the chat. `OK`: Will escalate the chat again. **Cancel**: Will prevent the chat escalation.	If the user presses the Ok button after the session expires then the chat escalation would fail. Upon refreshing the `chatframe.jsp` page thereafter would redirect the user to `chatsessionexpire.jsp` page.

Note: For a CIRS case and when action = redirect, after the `htmlclient.jsp` is refreshed, the page is redirected to a JSP page specified by `website.pages.login` metadata attribute. This attribute points to `account.jsp` in OOTB website.

Optional Configurations

Following configurations are optional. You can apply them as per your requirement.

Configuration related to performance upgrade of Poller and ICEmail Servers (Introduced in IC 7.3.3 FP)

To configure upper threshold, use SizeUpperThresh on the configuration tab of Poller/ICEmail in IC Manager. The default value of SizeUpperThresh is 1.5 GB. The maximum value that is accepted is 1.8 GB.

To configure lower threshold, use SizeLowerThresh on the configuration tab of Poller/ICEmail in IC Manager. The default value of SizeLowerThresh is 1 GB. The minimum value that is accepted is 500 MB.

The SizeUpperThresh must always be greater than SizeLowerThresh. The delta between the two thresholds must be in 10s of MB.

AllowCompleteWhileRinging Property declaration (Introduced in IC 7.3.3 FP)

Allows completion of consult/conference/transfer while the call is ringing at the other agent's end.

This can be configured using steps below.

1. Login to IC Manager.

2. Go to **Tools** > **Property Declarations**.

3. From **Property Section** select **Agent/Desktop/Voice**.

4. Add following property under this **AllowCompleteWhileRinging (Datatype - boolean)**.

5. Click **OK**.

6. Go to **Tools** > **Groups** and add the above properties under **Agent/Desktop/Voice**.

Email Template Administration (Introduced in IC 7.3.2 FP)

Table below describes additional parameters to control message delivery to ICEmail servers. The parameters can be modified in <AVAYA_IC73_HOME>\email \jsp\WEB-INF\web.xml file on the server where RL Manager is configured. The Email Template Administration service will need to be restarted for the changes to take effect.

Sr. No.	Configuration parameter	Default value	Mandatory?	Description
1	rlmanager.vesp.request.rejectchangerecordcounter	5	No	Controls how many times particular change record is resent to ICEmail

Sr. No.	Configuration parameter	Default value	Mandatory?	Description
				server in case of an error. In case ICEmail server faces DB error, RLManager tries to send same record. This can end up in a loop if ICEmail server does not recover from Database error. Use this configuration parameter to control how many times RLManager tries to send a particular record to ICEmail server.
2	rlmanager.vesp.request.retrycount	3	No	Controls how many times RLManager can retry to send VESP command to ICEmail server in case of CTI exceptions of type `CtiCommException,` `CtiDomainException,` `CtiObjectDoesNotExi` `stException,` `CtiResourceExceptio` `n.` In case of network failure between RLManager and ICEmail server, RLManager receives CTI exceptions.
3	rlmanager.vesp.request.retrytime	180000 milliseconds	No	RLManager uses a queue to deliver change record to ICEmail server. In case RLManager has to retry sending a change record, this record is pushed in this queue. This configuration parameter controls on how frequently retry of such change records are

Sr. No.	Configuration parameter	Default value	Mandatory?	Description
				to be sent.
4	rlmanager.recreateapi.requestcount	15	No	Controls on when to invoke `ICEmail.RecreateRLManager()` VESP API when there are numerous change records yet to be delivered to ICEmail server.
				If there are multiple unsent change records in RLManager's queue then this parameter decides when to discard those change records and call `ICEmail.RecreateRLManager()` VESP API. Refreshes everything in ICEmail server.

Synchronization of ICEmail in-memory template data (Introduced in IC 7.3.2 FP)

A mechanism is added in ICEmail server to synchronize its in-memory template data with DB. This is required if RL Manager and ICEmail updates get out of sync for some reason (like network connection problems etc.).

To enable the synchronization in ICEmail server, "`TemplRecreateGenUpdas`" parameter is introduced. It's default value is 1. This means on Generic Update, ICEmail server will synchronize its in-memory template data with DB.

To disable the default behavior, you can set "`TemplRecreateGenUpdas`" parameter to 0 in ICEmail Server configuration.

Enable logging of JSON tree sent to agent (Introduced in IC 7.3.2 FP)

The JSON tree that is sent to agent by ICEmail is logged when `TemplWriteToFile` is set to 1 on the configuration tab in ICEmail.

The JSON tree logs are written to `<AVAYA_IC73_HOME>/logs/EmailTemplateEncode.log`.

Setting `TemplWriteToFile` to 0, will be like the default behavior of not logging the JSON tree.

Both `TemplRecreateGenUpd` and `TemplWriteToFile`, can be set through Generic Update.

Configuration for Security Fixes (Introduced in IC 7.3.2 FP)

Security configurations for Website

The security fixes contain changes to the website configuration. Therefore, you must reconfigure the servers which host the website application. There are two ways in which this can be achieved:

- Rerun the configtool for website.

- Manual changes in the web.xml file.

Although it is better to rerun the configtool for website, customers might follow a manual approach to the same in case there are configuration changes done in `web.xml` file.

When Config Tool is run, the tool makes necessary changes the `web.xml`. For manual changes, perform the following steps:

1. Add and map the new security filter:

   a. Navigate to `<AVAYA_IC73_HOME>\comp\website\WEB_INF`.

   b. Edit `web.xml` file.

   c. Add the following lines after the SQL injection filter definition. See the template file in `<AVAYA_IC73_HOME>\bin\config\template` folder:

```
<filter>

          <description>This filter will validate the Request and Response. It
will also set HTTPOnly and secure cookies

          </description>

          <display-name>securityFilter</display-name>

          <filter-name>securityFilter</filter-name>

          <filter-class>com.quintus.security.SecurityFilter</filter-class>

          <init-param>

                  <param-name>httponly</param-name>

                  <param-value>true</param-value>

          </init-param>
```

```
            <init-param>

                    <param-name>redirectParams</param-name>

                    <param-value>aicRedirectURL</param-value>

            </init-param>

            <init-param>

                    <param-name>redirectOverride</param-name>

                    <param-value>true</param-value>

            </init-param>

            <init-param>

                    <param-name>validateParams</param-name>

                    <param-
value>aicEscRequestedMedia=chat,email,fax,callback,pvchat,ivchat</param-value>

            </init-param>

            <init-param>

                    <param-name>exceptions</param-name>

                    <param-value>chat_escalate</param-value>

            </init-param>

    </filter>

    <filter-mapping>

            <filter-name>securityFilter</filter-name>

            <url-pattern>/*</url-pattern>

    </filter-mapping>
```

2. Add Valve configuration:

   a. Navigate to `<AVAYA_IC73_HOME>\tomcat\conf` folder.

   b. Edit the server.website.xml file.

   c. Add the following lines after the Context definition. See the template file in
      `<AVAYA_IC73_HOME>\bin\config\template` folder:

      `<Valve className="org.tomcat.valves.sessionFixationValve" />`

Other security recommendations for Website

The following configurations are recommended for improving the security of Avaya IC application:

- Always deploy Public and Administration website on separate servers.

- Have the server hosting the Administration website behind the firewall.

- Always enable HTTPS and disable HTTP for webserver and the Tomcat application.

- Turn off folder browsing for the website on the webserver.

- Turn off Anonymous access to website related files/folders by the webserver application.

Note: Recommendations #1 & 2 helps secure IC website against the following vulnerability:

A malicious user that can guess the path to the web interfaces can potentially guess or brute force a password to gain administrative control of the application.

Configuration for the IIS to deny requests containing sensitive URLs

The changes are related to have IIS deny requests containing sensitive URLs. For example, by default IIS restricts all requests trying to serve content from the 'bin' folder. However, as WEB-INF is a Tomcat thingy, we will need to specifically tell IIS to not to serve these URLs. Here are screenshots for the same:
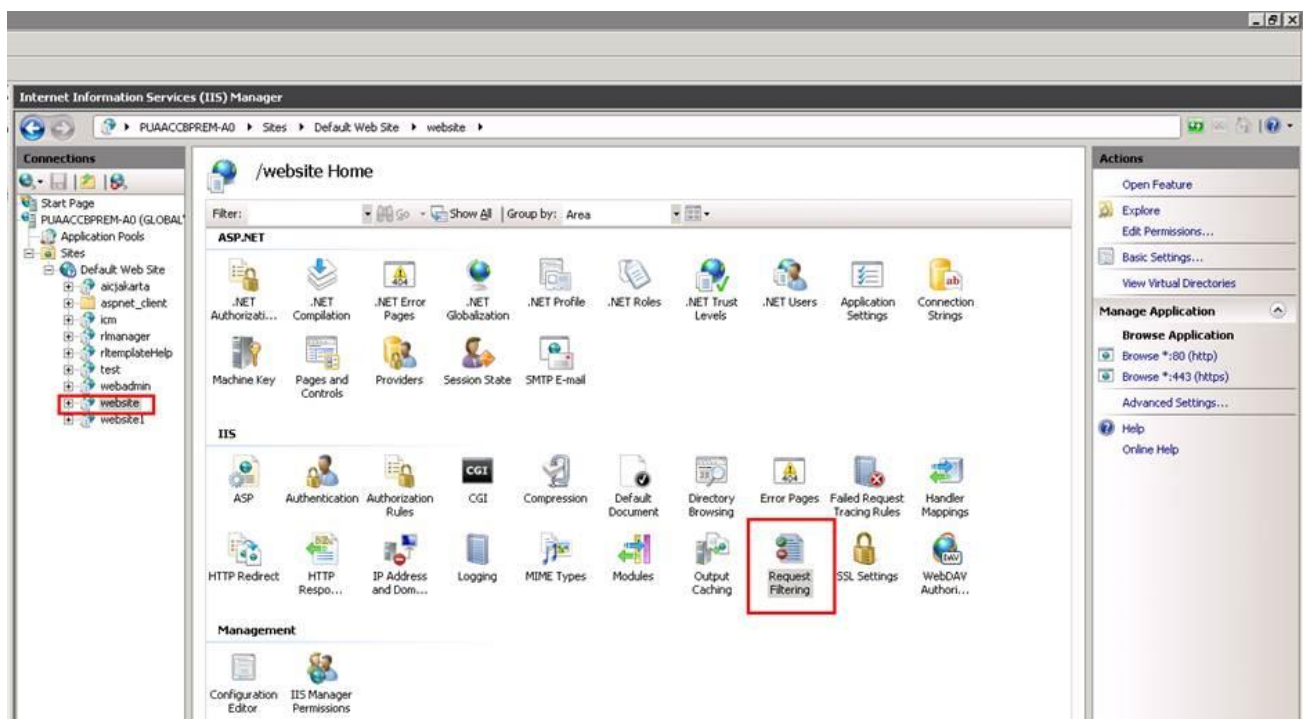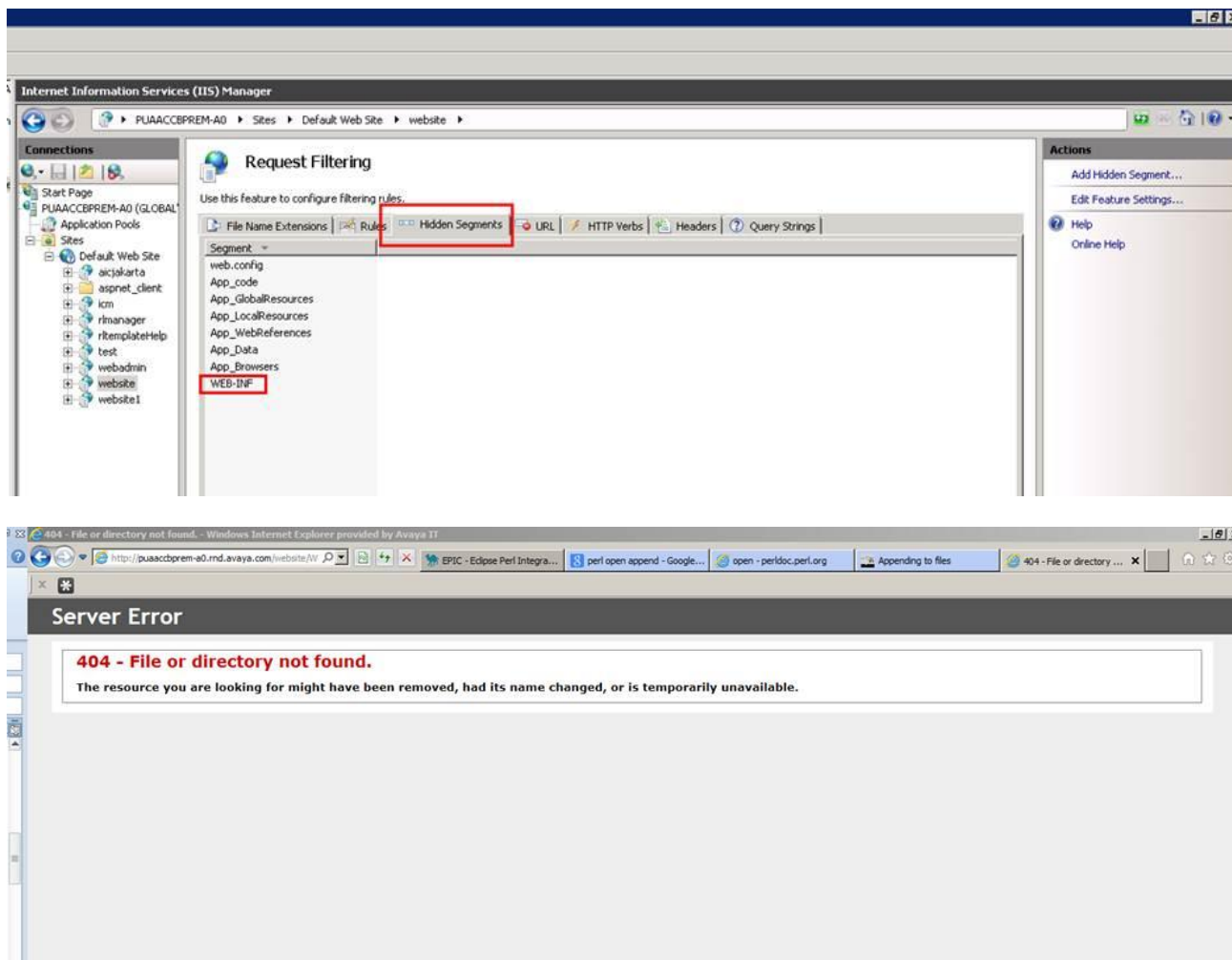
Again, some JS (static) and css files are served by IIS, and hence the Tomcat filter does not come into effect, therefore the headers are not present.

However, we do not really need this header in case of content without frames, so this is not really an issue.

Configuration of RONA AUX Reason code for Business Advocate (Introduced in IC 7.3.2 FP)

TS do not use any specific reason code for a RONA call with Advocate. TS uses the default AUX reason code configured in the TS configuration. This might create issues for reporting, since the default AUX reason code might not be desired for RONA calls.

The new feature would enable TS to use a configured `AUX reason code for RONA` in the RONA scenario. This would help in isolating the calls that RONAed based on the reason code.

Note: This feature is supported with all clients except Siebel hybrid and native client.

Steps to configure AUX reason code to be used in case of RONA:

1. In IC Manager, open TS configuration and navigate to the TS server tab.

2. Right-click and enable the advanced properties.

3. In the Rona Reason code, select a reason code. The reason code selected here should be preconfigured under codes, in the IC Manager.

4. Ensure that the value set in Agent/Desktop/AuxRonaReasonCode is in sync with the Rona code entered in TS configuration.

5. Restart the TS server.

Configuration for Inactivity timeout for Chat Disconnect (Introduced in IC 7.3.2 FP)

A provision is added to the OOTB IC public website wherein the ongoing live chat between the customer and the Agent is automatically disconnected in case the customer inactivity crosses the disconnect time set. This functionality is applicable for **Chat** as well as for **Chat and Callback** of IC public website.

To add the metadata properties for the above feature perform the following:

1. In a Web browser, navigate to the IC Website Administration page:
   `http://<server_name>/website/admin/login.jsp`.

2. Enter the user name and password and click **Next** to log in to the IC Website administration page.

3. Access the add metadata page:
   `http://<server_name>/website/admin/tenancy/addmd.jsp`.

4. Add the following metadata properties:

   - Metadata name = `chat.htmlclient.customer.inactivitytimer.enabled`.

   - Default value = false.

   - Description = This flag determines whether chat inactivity timer is enabled or is disabled. Valid values are true/false.

   - Tenant Property(checked)

5. Click **Add Metadata**.

6. Add the following metadata properties:

   Metadata name = `chat.htmlclient.customer.inactivity.totaltime`.

   Default value = 10

   Description = Total time (in minutes) that an active ongoing chat can continue without getting disconnected owing to customer inactivity. Minimum value can be 1 minute.

Tenant Property(checked)

7. Click **Add Metadata**.

8. Add the following metadata properties:

   - Metadata name = `chat.htmlclient.customer.inactivity.countdowntime.`

   - Default value = 60,10

   - Description = The first value, in seconds, determines the time duration for which a inactivity warning message would be displayed to the customer. Default is 60 seconds.

   - The second value, in seconds, determines the duration for which the countdown timer changes color to signify that chat disconnection time is closing upon. Default is 10 seconds.

   - Tenant Property(checked)

9. The following property is optional and is only used if Chat Inactivity feature needs to be enabled for **Join Us** customers as well.

10. Click **Add Metadata**.

11. Add the following metadata properties:

    - Metadata name = `chat.htmlclient.customerjs.inactivitytimer.enabled.`

    - Default value = false

    - Description = This flag determines whether chat inactivity timer is enabled or is disabled for **Join Us** customer. Valid values are true/false.

    - Tenant Property(checked)

12. In case the above tenant values require change, then the change can be from the IC Multitenant administration page.

13. Traverse to `http://<server_name>/website/admin/index.jsp` page and select **IC website Multi Tenant Administration**.

14. Click **Tenant Properties** and select the appropriate tenant.

15. Click **chat**.

16. Search for following metadata chat property and make appropriate changes to their values.

    - `chat.htmlclient.customer.inactivitytimer.enabled`

    - `chat.htmlclient.customer.inactivity.totaltime`

    - `chat.htmlclient.customer.inactivity.countdowntime`

    - `chat.htmlclient.customerjs.inactivitytimer.enabled`

Note: if `chat.htmlclient.customerjs.inactivitytimer.enabled` is set to true then `chat.htmlclient.customer.inactivitytimer.enabled` has to be true also.

17. Click **Update Data** set the above tenant property values.

Note:

- Even if the agent is actively chatting but the customer is not typing in anything, then such a chat can be disconnected after the customer inactivity time crosses the disconnect interval

- This feature is only available for chat only and does not support the case where the customer is simultaneously using cobrowse/collaboration. In such a scenario the customer still has to press in any key to keep the chat active.

- The above feature is useful only in case where customer wants a disconnection feature on the customer end and customer does not use the collaboration/cobrowse feature.

Allowing non-RFC compliant emails to be processed by AIC (Introduced in IC 7.3.2 FP)

From IC 7.3 onwards, the Poller server checks email headers, From/Sender/ReplyTo, for RFC compliance. By default, if none of these headers are compliant to RFC then such an email remains on the email server and the Poller server alarms every polling interval about this email until the email is cleared from the mailbox. To disable or enable RFC compliance, a new configuration value for the Poller server is provided as follows.

Allowing Poller Server to download NON-RFC compliant emails to into the system

(NON-RFC compliance is based on invalid from/sender/reply-to addresses)

1. Log in to IC Manager using admin account.

2. Click the **Server** tab.

3. Double-click the **Poller** server.

4. Click the **Configuration** tab.

5. Add a new Couple with name: `DisableEmailAddressRFCCheck`.

6. Values are:

   - 1 - Turn OFF RFC compliant checking.

   - 0 - Turn ON RFC compliant checking.

Note: Not adding this value or adding any value apart from 1 will enable this feature.

Such emails with invalid from/sender/reply-to addresses is bounced by the SPAM plugin of the Poller server through the email server to the bounce address of the respective Mail Account from which the email was polled. Unless the flag `DisableRFCCheckInSpamPlugin`, mentioned in following point, 2 is used.

7. Click **OK**.

8. Restart the **Poller** server.

Configuring the Poller server to allow NON-RFC compliant emails to be delivered to agent

1. Click the **Server** tab.

2. Double-click the **Poller** server.

3. Click the **Configuration** tab.

4. Add a new Couple with:

   - Name: `DisableRFCCheckInSpamPlugin`.

   - Values are:

     – 1 - Turn OFF SPAM RFC checking.

     – 0 - Turn ON SPAM RFC checking.

Note: Not adding this value or adding any value apart from 1 will enable this feature.

5. Click **OK**.

6. Restart the **Poller** server.

Non-RFC compliance is based on invalid from/sender/reply-to addresses.

Configuring a substitute email address which will be shown to the agent

Substitute email address is used in place of FROM address of the incoming email in case the email MIME does not contain FROM address or contains an invalid one.

1. Click the **Server** tab.

2. Double-click the **Poller** server.

3. Click the **Configuration** tab.

4. Add a new Couple with:

   - Name: SubstitueFromAddress.

   - Value: Any valid email address.

Note: If email address is not provided or an invalid email address is provided, the respective polling account's bounce email address is used as a substitute address.

5. Click **OK**.

6. Restart the **Poller** server.

New Connection properties for SDK login issue (Introduced in IC 7.3.2 FP)

SDK agents cannot login after network issue. To resolve this issue, you can configure the following properties in `web.xml`:

- `basicservices.cacherefreshattempt`

  Specifies the maximum number of attempts to retrieve the data from DB if there are problems while retrieving data. The default value is 60 attempts.

- `basicservices.cacherefreshinterval`

  Specifies the interval in milliseconds between two attempts. The default value is 1000 milliseconds.

Disabling the Chat time stamp for the AARC (Introduced in IC 7.3.2 FP)

OOTB the chat transcripts are displayed with the time stamp but if the Agent wants to disable it then the following property must be set to false in the `Application.properties` file located `<AARC_HOME>\webagent`:

`chat.enable.timestamp=false`

Optional Security Configuration for IC Public Website for Modern day browsers (Introduced in IC 7.3.1 SP)

Note: These changes are not applicable to IC 7.3.2 FP and onwards.

Modern day browsers like Microsoft Internet Explorer 8, Microsoft Internet Explorer 9 (32-bit only), Google Chrome 21, and others have implemented security enhancements including **Clickjacking Defense**. This implementation can result in the website not being accessible when frames are used. IC website can be secured against such attacks by adding a new element in `web.xml` file.

Perform the following steps on the computers where website is installed. This is applicable for all operating systems. If the admin and public websites are configured on separate computers, perform this for the public website.

1. Stop website service.

2. Browse to the following folder on the computer where the website is installed:
   `<AVAYA_IC73_HOME>/comp/website/WEB-INF` and backup the `web.xml` file.

3. Open the `web.xml` file for editing.

4. Add the element as highlighted:

```
<servlet>

        <servlet-name>

            InitServlet

        </servlet-name>

        <servlet-class>com.quintus.servlet.InitServlet</servlet-class>
...........

...........

    <init-param>

            <param-name>xFrame</param-name>

            <param-value>SAMEORIGIN</param-value>

     </init-param>
<load-on-startup>1</load-on-startup>

        </servlet>
```

5. Delete the folder `<AVAYA_IC73_HOME>/tomcat/work/Catalina/localhost/website` for cleaning tomcat cache.

6. Start the website service.

Optional Security Configuration to prevent SQL Injection attack on IC Admin Website (Introduced in IC 7.3.1 SP)

A new filter, `sqlAttackFilter`, must be activated as part of the website configuration. This activation guards against any SQL injection attacks on the Admin website.

This attribute represents a group of SQL keywords. If these attributes are encountered in the http request stream, they would be blocked from being executed on the server.

`<param-name>sqlAttackPattern</param-name>`

By default, all the admin websites pages other than the ones mentioned as part of `sqliByPassURLPattern` init parameter would be checked against these key words for possible SQLI attacks. If a potential SQL Injection attack is detected the session is invalidated and error page is displayed.

There are two parameters:

- `<param-name>sqlHTTPAttackString</param-name>`

This parameter indicates which all URL patterns of the admin website must be bypassed for detection of SQLI attacks. These admin pages URL with the listed patterns, when detected, can only be checked against the `sqlHTTPAttackString` parameter values.

- `<param-name>sqliByPassURLPattern</param-name>`

  The URLs, which are mentioned as part of the `sqliByPassURLPattern` init parameter, can only be tested for these HTTP SQL attack strings.

Perform the following steps on the computers where website is installed. This is applicable for all operating systems. If the admin and public websites are configured on separate computers, perform this for the admin website.

1. Stop website service.

2. Browse to the following folder on the computer where website is installed: `<AVAYA_IC73_HOME>/comp/website/WEB-INF` and backup the `web.xml` file.

3. Open the `web.xml` file for editing.

4. Add the element as highlighted:

```
<filter>

            <description>This filter is used to detect SQLI.</description>

            <display-name>sqlAttackFilter</display-name>

            <filter-name>sqlAttackFilter</filter-name>

            <filter-class>com.quintus.security.sqlAttackFilter</filter-class>


            <init-param>

            <param-name>sqlAttackPattern</param-name>

            <param-value> create, alter, drop, rename, select, insert, update,
delete, grant, revoke,@@version, exec, union, waitfor, order by, case when,
utl_,  winhttp</param-value>

            </init-param>

            <init-param>

            <param-name>sqlHTTPAttackString</param-name>

            <param-value> utl_, winhttp</param-value>

            </init-param>

            <init-param>
```

```
            <param-name>sqliByPassURLPattern</param-name>

            <param-
value>category=account,category=escalate,category=website</param-value>

            </init-param>

    </filter>

    <filter-mapping>

            <filter-name>sqlAttackFilter</filter-name>

            <url-pattern>/admin/*</url-pattern>

    </filter-mapping>
```

5. Delete folder `<AVAYA_IC73_HOME>/tomcat/work/Catalina/localhost/website` for cleaning tomcat cache.

6. Start website service.

Siebel AICD Server Logging (Introduced in IC 7.3.1 SP)

Siebel AICD logging is enhanced to let you configure file count and file size. These parameters are configured in the AICD.ini file.

To increase log file size and log file count perform the following:

1. Ensure the shutdown of the Communications Session Manager component from the Siebel Server Administration screen.

2. Open the AICD.ini file from the bin folder of the Siebel Server or the location of the AICD installation in any text editor like Notepad.

3. Add the section following the Version section in the AICD.ini file. The values specified below are given as examples. You can replace them with any other numeric values according to your requirements. The file size is measured in bytes here.

    ```
    [SiebelAICDLog]

    FileCount = 5

    FileSize = 25000000
    ```

4. Save and close the AICD.ini file.

5. Start the Communications Session Manager component from the Siebel Server Administration screen.

Note: The default values used when these parameters are not configured are:

```
FileCount = 2

FileSize = 2000000
```

Chat Transcript Configuration (Introduced in IC 7.3.1 SP)

Refer description of this configuration above in "Viewing Chat Transcript" section. To make the configuration changes follow the given instructions:

1. Stop the IC Website service on the IC server where website is deployed.

5. Navigate to the `<AVAYA_IC73_HOME>\tomcat\work\Catalina\localhost\` folder and delete the folder 'website'.

6. Browse to "`<AVAYA_IC73_HOME>\comp\website\admin\wtc\`" and open `transcript.jsp`

7. Locate the following statement: `int defaultNTaskID = 200;`

8. Change the value from 200 to any value between 1 and 1000.

9. Save and close `transcript.jsp`.

10. Start the IC Website service on the IC server where website is deployed.

Configuration related to ICM Server and CIRS Log files (Introduced in IC 7.3.1 SP)

Refer description of this configuration above in "Changes to ICM Server and CIRS Log files" section. Perform the following steps to set the maximum log file size of the `icmserver.log` for the ICM server:

1. Log in to the IC Manager and go to the **Configuration** tab.

2. Select **Chat**. After the tree expands, select **ICM** under Chat.

3. Select **New** to define a new ICM configuration or select an existing ICM to edit.

4. Right-click the configuration page and select **Show Advanced properties**.

5. Change the value of **Maximum ICM Log Size (in KB)** parameter to desired value greater than 10240.

Note: Ensure that the ICM global name specified here is the same as the dsObjectName of the `SystemParms.txt` file. For more information, see the IC 7.3 Installation and Configuration guide. If you need to specify a different ICM value for the **Maximum ICM Log size (KB)** parameter for different servers, then create a separate IC Manager configuration in IC Manager with unique global name.

Web Form Design for Collaborative Form Filling (Introduced in IC 7.3.1 SP)

The Collaborative Form Filling feature enables the customer and the agent to collaborate and fill forms on the web pages that are pushed by either the customer or the agent.

The web page forms for the Collaboration feature must meet the following design guidelines:

1. HTML `<!DOCTYPE>` declaration must be present in the HTML document in which the form is present.

2. The form must be inside an HTML body tag.

3. It is mandatory to have the elements inside an HTML Form tag.

4. Every element must have a unique ID except radio button.

5. In case of a radio button, every sub-element must have unique name.

Note: These guidelines are not specific to SP 7.3.3 and apply to all version of IC.

The earlier design guidelines are as follows:

```
<!DOCTYPE html>

<html>

<head>

<!--  This is example only. Consult your web designer for designing web page -->

</head>

<body>

<form action="back-end script" method="posting method">

          <!--   Form must be encapsulated within begin and end of body tag --
>

          <!--   Input elements must be encapsulated within begin and end of
form tag -->

          <!--   Every element must have unique id -->

          <!--   Radio button sub-element must have unique name -->

</form>

</body>

</html>
```

The ResetScriptIteration setting for WACD (Introduced in IC 7.3.1 SP)

With this feature, when the WACD server is restarted, WACD maintains the same priority and same workgroup for email contacts that it had prior to the restart, rather than resetting the priority of tasks.

However, enabling of this new behavior depends on the parameter ResetScriptIteration and pushing the new script to the database.

Note: The parameter ResetScriptIteration is applicable only for the email contacts. If you are not using the email channel, then the following configurations can be skipped.

The following steps must be performed, only if the new behavior is required. Otherwise, skip steps 1 to 6.

Configuration steps to be performed after installing IC 7.3.1 SP:

1. If the new behavior of WACD server is required, perform the following steps for all WACD servers:

   a. Login to IC Manager.

   b. Go to the **Server** tab and double click on a **WACD** server to edit the configuration.

   c. Go to the **configuration** tab and add a new configuration parameter:

      − Name: ResetScriptIteration

      − Value: 0

   d. Click **OK** to save the WACD configuration.

2. Gathering database information.

   a. Log in to IC Manager.

   b. Open **Tools** menu and click on **IC Data Sources...**.

   c. In **IC Data Sources...** dialog box opens expand interaction_center.

   d. Click on ccqDBConnection.

   e. Note down Database Name and Database Server Values.

3. Update the `w_script_details` table:

   ▪ If the CCQ DB is of type SQL Server or DB2, execute the SQLDB2 Script given in the table below.

   ▪ If the CCQ DB is of type Oracle, execute the ORACLEDB script given in the table below.

4. After executing the query, from IC Manager restart the WACD server.

- If the parameter is set to 1, WACD behaves as it used to, before the fix. For example, queue scripts starts from iteration zero. Priorities of tasks are reset.

- If the parameter is set to 0, WACD recreates tasks at the same priority and workgroup that it had prior to the restart provided the new script is uploaded by following steps 1 to 6. Priorities are maintained as prior to restart.

5. By default, the WACD server considers the value of 'ResetScriptIteration' parameter to be 0 unless the value is explicitly set to 1 in the WACD configuration in IC Manager.

Note: Copy the text of the following script into a Rich Text Editor like MS Word to preserve the formatting. Copying the text directly into SQL Query Admin tool might lead to functional issues if the content gets modified including extra space or removal of space unintentionally.

SQLDB2 Script

```
update w_scripts_detail set script_text =''' This is the default script

''

'' It looks for the following key-values

''

'' Expectedqueuetime

'' - If present, it will display the expected

'' hold time

''

'' Workgroup

'' - The value should be a Workgroup to enqueue

'' to

''

'' Agent

'' - The value should be an agent name to

'' enqueue to

''

'' Priority

'' - The priority of an enqueue (team or

'' agent)
```

```
''

'' Say

'' - A string message to say to the customer

''

'' PushURL

'' - A URL to push to the customer

''

'' Wait

'' - A value (in secs) to wait before

'' processing the next set of keys

''

'' If Expectedqueuetime is defined, get

'' the expected hold time

if acd.GetValue("Expectedqueuetime") <> "0" then

acd.sv("time", ACD.ExpectedQueueTime(10))

if acd.gv("time") = 0 then

say("An agent will be with you shortly.")

endif

if acd.gv("time") <> -1 then

say("Your approximate wait time is " & acd.gv("time") & " minutes.")

endif

endif

'' First check if pacAgentName is provided. If so, this will be

'' used first, and the main loop only entered if the requested

'' agent does not become available within 30 seconds

if acd.GetValue("pacAgentName") <> "0" then

acd.GetAgent(acd.GetValue("pacAgentName")).Enqueue()

Say("Agent " & acd.GetValue("pacAgentName") & " will be with you shortly.")
```

```
Sleep(30)

endif

acd.sv("exit", 0)

''

'' Start the loop

''

while (acd.gv("exit") = 0)

acd.sv("exit", 1)

''

'' Check to see if a team is defined

'' and if so, check for a priority

''

if acd.GetValue("Workgroup" & acd.gv("cnt")) <> "0" then

if acd.GetValue("Priority" & acd.gv("cnt")) <> "0" then

if acd.GetValue("Priority" & acd.gv("cnt")) = "low" then

ACD.GetTeam(acd.GetValue("Workgroup" & acd.gv("cnt"))).Enqueue(low)

endif

if acd.GetValue("Priority" & acd.gv("cnt")) = "normal" then

ACD.GetTeam(acd.GetValue("Workgroup" & acd.gv("cnt"))).Enqueue(normal)

endif

if acd.GetValue("Priority" & acd.gv("cnt")) = "high" then

ACD.GetTeam(acd.GetValue("Workgroup" & acd.gv("cnt"))).Enqueue(high)

endif

if acd.GetValue("Priority" & acd.gv("cnt")) = "urgent" then

ACD.GetTeam(acd.GetValue("Workgroup" & acd.gv("cnt"))).Enqueue(urgent)

endif

else

ACD.GetTeam(Cstr(acd.getvalue("Workgroup" & acd.gv("cnt")))).Enqueue()
```

```
endif

acd.sv("exit",0)

endif

''

'' Check to see if an agent is defined

'' and if so, check for a priority

''

if acd.GetValue("Agent" & acd.gv("cnt")) <> "0" then

if acd.GetValue("Priority" & acd.gv("cnt")) <> "0" then

if acd.GetValue("Priority" & acd.gv("cnt")) = "low" then

ACD.GetAgent(acd.GetValue("Agent" & acd.gv("cnt"))).Enqueue(low)

endif

if acd.GetValue("Priority" & acd.gv("cnt")) = "normal" then

ACD.GetAgent(acd.GetValue("Agent" & acd.gv("cnt"))).Enqueue(normal)

endif

if acd.GetValue("Priority" & acd.gv("cnt")) = "high" then

ACD.GetAgent(acd.GetValue("Agent" & acd.gv("cnt"))).Enqueue(high)

endif

if acd.GetValue("Priority" & acd.gv("cnt")) = "urgent" then

ACD.GetAgent(acd.GetValue("Agent" & acd.gv("cnt"))).Enqueue(urgent)

endif

else

ACD.GetAgent(Cstr(acd.getvalue("Agent" & acd.gv("cnt")))).Enqueue()

endif

acd.sv("exit",0)

endif

''

'' check for a say value
```

```
''

if acd.GetValue("Say" & acd.gv("cnt")) <> "0" then

say(acd.getvalue("Say" & acd.gv("cnt")))

acd.sv("exit",0)

endif

''

'' check for a push url value

''

if acd.GetValue("PushURL" & acd.gv("cnt")) <> "0" then

pushurl(acd.getvalue("PushURL" & acd.gv("cnt")))

acd.sv("exit",0)

endif

''

'' check for a wait value

''

if acd.GetValue("Wait" & acd.gv("cnt")) <> "0" then

acd.setvalue("sleep", acd.getvalue("Wait" & acd.gv("cnt")))

sleep(Int(CDbl(acd.getvalue("sleep"))))

acd.sv("exit",0)

endif

''

'' If this was the 1st time through and

'' no values were set, then we need to do

'' a normal routing.

''

''

if acd.gv("exit") = 1 AND acd.gv("cnt") = 0 then

say("Please wait for the next available eContact agent.")
```

```
while(true)

''ACD.GetTeam("Default").Enqueue()

Sleep(30)

Say("Please continue to wait...")

wend

endif

''

''

'' If any values were set for this count

'' then up the counter and continue,

'' otherwise, set the counter back to zero

'' and start over.

''

if acd.gv("exit") = 0 then

acd.sv("cnt", acd.gv("cnt") + 1 )

else

acd.sv("cnt", 0)

endif

acd.sv("exit", 0)

wend'

where script_name='DefaultQueueScript';
```

ORACLEDB Script

```
set scan off;

declare sScriptVar varchar2(32767) := ''' This is the default script

''

'' It looks for the following key-values

''
```

```
'' Expectedqueuetime

'' - If present, it will display the expected

'' hold time

''

'' Workgroup

'' - The value should be a Workgroup to enqueue

'' to

''

'' Agent

'' - The value should be an agent name to

'' enqueue to

''

'' Priority

'' - The priority of an enqueue (team or

'' agent)

''

'' Say

'' - A string message to say to the customer

''

'' PushURL

'' - A URL to push to the customer

''

'' Wait

'' - A value (in secs) to wait before

'' processing the next set of keys

''

'' If Expectedqueuetime is defined, get

'' the expected hold time
```

```
if acd.GetValue("Expectedqueuetime") <> "0" then

acd.sv("time", ACD.ExpectedQueueTime(10))

if acd.gv("time") = 0 then

say("An agent will be with you shortly.")

endif

if acd.gv("time") <> -1 then

say("Your approximate wait time is " & acd.gv("time") & " minutes.")

endif

endif

'' First check if pacAgentName is provided. If so, this will be

'' used first, and the main loop only entered if the requested

'' agent does not become available within 30 seconds

if acd.GetValue("pacAgentName") <> "0" then

acd.GetAgent(acd.GetValue("pacAgentName")).Enqueue()

Say("Agent " & acd.GetValue("pacAgentName") & " will be with you shortly.")

Sleep(30)

endif

acd.sv("exit", 0)

''

'' Start the loop

''

while (acd.gv("exit") = 0)

acd.sv("exit", 1)

''

'' Check to see if a team is defined

'' and if so, check for a priority

''

if acd.GetValue("Workgroup" & acd.gv("cnt")) <> "0" then
```

```
if acd.GetValue("Priority" & acd.gv("cnt")) <> "0" then

if acd.GetValue("Priority" & acd.gv("cnt")) = "low" then

ACD.GetTeam(acd.GetValue("Workgroup" & acd.gv("cnt"))).Enqueue(low)

endif

if acd.GetValue("Priority" & acd.gv("cnt")) = "normal" then

ACD.GetTeam(acd.GetValue("Workgroup" & acd.gv("cnt"))).Enqueue(normal)

endif

if acd.GetValue("Priority" & acd.gv("cnt")) = "high" then

ACD.GetTeam(acd.GetValue("Workgroup" & acd.gv("cnt"))).Enqueue(high)

endif

if acd.GetValue("Priority" & acd.gv("cnt")) = "urgent" then

ACD.GetTeam(acd.GetValue("Workgroup" & acd.gv("cnt"))).Enqueue(urgent)

endif

else

ACD.GetTeam(Cstr(acd.getvalue("Workgroup" & acd.gv("cnt")))).Enqueue()

endif

acd.sv("exit",0)

endif

''

'' Check to see if an agent is defined

'' and if so, check for a priority

''

if acd.GetValue("Agent" & acd.gv("cnt")) <> "0" then

if acd.GetValue("Priority" & acd.gv("cnt")) <> "0" then

if acd.GetValue("Priority" & acd.gv("cnt")) = "low" then

ACD.GetAgent(acd.GetValue("Agent" & acd.gv("cnt"))).Enqueue(low)

endif

if acd.GetValue("Priority" & acd.gv("cnt")) = "normal" then
```

```
ACD.GetAgent(acd.GetValue("Agent" & acd.gv("cnt"))).Enqueue(normal)

endif

if acd.GetValue("Priority" & acd.gv("cnt")) = "high" then

ACD.GetAgent(acd.GetValue("Agent" & acd.gv("cnt"))).Enqueue(high)

endif

if acd.GetValue("Priority" & acd.gv("cnt")) = "urgent" then

ACD.GetAgent(acd.GetValue("Agent" & acd.gv("cnt"))).Enqueue(urgent)

endif

else

ACD.GetAgent(Cstr(acd.getvalue("Agent" & acd.gv("cnt")))).Enqueue()

endif

acd.sv("exit",0)

endif

''

'' check for a say value

''

if acd.GetValue("Say" & acd.gv("cnt")) <> "0" then

say(acd.getvalue("Say" & acd.gv("cnt")))

acd.sv("exit",0)

endif

''

'' check for a push url value

''

if acd.GetValue("PushURL" & acd.gv("cnt")) <> "0" then

pushurl(acd.getvalue("PushURL" & acd.gv("cnt")))

acd.sv("exit",0)

endif

''
```

```
'' check for a wait value

''

if acd.GetValue("Wait" & acd.gv("cnt")) <> "0" then

acd.setvalue("sleep", acd.getvalue("Wait" & acd.gv("cnt")))

sleep(Int(CDbl(acd.getvalue("sleep"))))

acd.sv("exit",0)

endif

''

'' If this was the 1st time through and

'' no values were set, then we need to do

'' a normal routing.

''

''

if acd.gv("exit") = 1 AND acd.gv("cnt") = 0 then

say("Please wait for the next available eContact agent.")

while(true)

''ACD.GetTeam("Default").Enqueue()

Sleep(30)

Say("Please continue to wait...")

wend

endif

''

''

'' If any values were set for this count

'' then up the counter and continue,

'' otherwise, set the counter back to zero

'' and start over.

''
```

```
if acd.gv("exit") = 0 then

acd.sv("cnt", acd.gv("cnt") + 1 )

else

acd.sv("cnt", 0)

endif

acd.sv("exit", 0)

wend';

begin

update qw_text set text=sScriptVar where qwkey=1;

end;
```

Enabling fullcore on AIX

"fullcore" will increase the size of each core file written on the system by including additional
information such as shared memory segments that might be needed in order to find the cause of a
problem, and additional data needed when debugging multi-threaded programs.

1. Check if the "fullcore" flag is on:

    ```
    # lsattr -E -l sys0 -a fullcore
    fullcore false Enable full CORE dump True
    ```

2. Set the flag to "true":

    ```
    # chdev -l sys0 -a fullcore=true
    sys0 changed
    ```

Configuring variable number of Wrapup code types (Introduced in IC 7.3.4 SP)

A.   Adding wrapup code types using IC manager

1. Login into IC Manager using Admin account
2. Open the code Manager by using codes menu
3. Populate the wrapup codes
4. Select the existing category code for example DefaultCategoryCode
    Note : The implementation is not applicable for Generic Codes . We would be analyzing it as
    AARC does not load Generic codes.
5. Right click and select New to add new code type.

6. Add the required information for all 3 fields. (For example TestCodeType1)
7. Click on Apply/OK button
8. Now select the newly added code type i.e. TestCodeType1
9. Right click and select the New to add code values
10. Add the required information for all 3 fields.
11. Click on Apply/OK button
12. Open repository database and make sure that new codes are added in Classificationcode, classificationgrp and localizedcode table
13. Perform the step 4 to 13 for adding more code types and values
Refer following diagram for adding wrapup code type and wrapup code value.
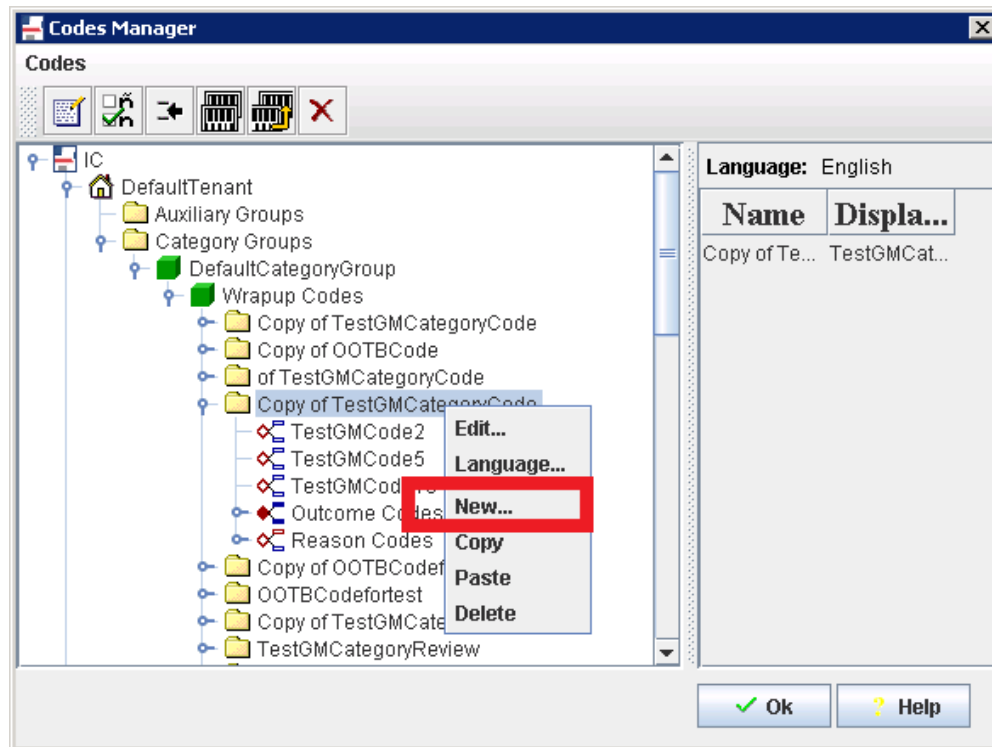
B.   Operations for Wrapup Code Types using IC manager

Context Menu for Wrapup Code Type

1. Edit – Modifying the selected wrapup code type

2. Language – Setting the language for display values.

3. New – Providing the option for adding new wrapup code values for selected wrapup code type.

4. Copy – Copying the code type from one category to another category or same category.

5. Paste – Allowing paste of wrapup code values which are selected from same wrapup code type or different code type.

6. Delete – Allow to delete the selected wrapup code type.

Context Menu for Wrapup Code Node

1. Edit – Modifying the selected wrapup code Node

2. Language – Setting the language for display values.

3. Copy – Copying the code value from one wrapup code type to another wrapup code type or in the same wrapup code type.

4. Delete – Allow to delete the selected wrapup code node.

C.   Wrapup Dialog:

To use variable number of wrapup codes in AARC please perform the following steps:

- ▸ Enable wrapup property from IC manager

- ▸ Specify the DefaultCategoryGroup and DefaultTenant in IC manager

- ▸ Launch AARC with any channel enabled. For example voice

- ▸ Give a call to an agent.

- ▸ Complete the contact.

- ▸ WrapUp dialog is displayed with the variable number of code types

- ▸ Select the category and corresponding code values and add into the selection box by using Add button

- ▸ You can select the multiple selection by using different combinations or using another category

- ▸ Wrap the contact

- ▸ All selected wrapup code types are saved in taskperformed table.

If the wrapup code types are more than 3, use the scroll bar to view and select from the other code types.

Chapter 5: Uninstall program

The Avaya IC 7.3.4 installation program installs an uninstall program that can remove the files from the IC 7.3.4 installation. The program also returns your system to the previous state. If the installation fails, you must run the uninstall program before attempting to rerun the Installation program. Running the uninstall program preserves the files.

When the FP installer fails to complete the installation, any one of the following events might occur based on the progress achieved during installation:

- The uninstaller is created:

  You must run the uninstaller to remove the FP to restore the system to its original state.

- The uninstaller is not created:

  When the uninstaller is not created, it implies that the FP installer has already rolled back all the changes made to the system during installation. In this case, no action is required from the user.

Before running the Uninstall program

Before uninstalling IC 7.3.4 SP, ensure that no instance of IC Java or Tomcat is running.

1. For uninstalling servers, stop all servers using the procedures described in Stop IC services and Stop IC servers.

2. Exit the Agent and IC Manager applications on the system.

Note: On the AIX platform, you must end the processes that use the Rogue Wave binary files installed on the system.

Perform the following steps before uninstalling the AIX platform:

- Change folder to `$AVAYA_IC73_HOME/lib`.

- At the command prompt, type the following command: `slibclean`.

- At the command prompt, type the following command:

  - `fuser -k lib*12d*.a`

  - `fuser -k lib*.so`

- After running the `fuser -k lib*12d*.a` and `fuser -k lib*.so` commands, type the following at the command prompt:

- ▪ `fuser lib*12d*.a`

- ▪ `fuser lib*.so`

- No process IDs must be displayed in the results after running this command. However, even if one process ID is displayed in the results, you must restart the AIX computer.

Uninstalling IC 7.3.4

Perform the following steps on a system from where you want to uninstall IC 7.3.4 files:

1. Navigate to the following folder:

   - ▪ Windows：
     `...\IC73\ICServicePacks\7.3.4\<FolderNameOfComponent>\Record\`

   - ▪ Solaris and AIX:
     `.../IC73/ICServicePacks/7.3.4/<FolderNameOfComponent>/Record/`

2. Start the Uninstall program:

Windows

Double-click the uninstall7.3.4.bat file.

Solaris, AIX (server only) and Linux (server only)

1. At the command prompt, type: `./uninstall7.3.4.sh.`

2. Press **Enter**.

3. On the Welcome screen, click **Next**.

4. The next screen indicates the folder from which the files are uninstalled.

5. Click **Next** to start the Uninstall program which:

   - ▪ Restores the component to its previous state and displays confirmation of a successful uninstallation with a list of uninstallation warnings and errors that were encountered.

6. Click **Finish** if the uninstallation is successful.

On the Windows platform, restart the computer for the system to be restored to its previous state. AIX systems do not require restarting the computer.

Note: After the uninstallation is complete, sometimes the uninstall program does not delete the 7.3.x. The x is the SP number for which the uninstall program is executed. In such a case, you need to manually delete the 7.3.x subfolder from the `.../IC73/ICServicePacks` folder.

Uninstallation using the Silent command line option

The IC 7.3.4 Service Pack components can be uninstalled using the Silent command line option. When you run uninstallation in silent mode, the user interface is unavailable.

Silent mode

In a silent mode, rerun the same uninstallation in silent mode on another computer using the inputs from this text file.

To rerun the uninstaller in silent mode perform the following:

1. From the command prompt, go to the following folder:

Operating System	Folder name
Windows	`...\IC73\ICServicePacks\7.3.4\<FolderNameOfComponent>\Record`
Solaris and AIX	`.../IC73/ICServicePacks/7.3.4/<FolderNameOfComponent>/Record`
Linux	`IC Side: .../IC73/Uninstall_AICLinux7.3` `Siebel Side: $SIEBEL_HOME/Uninstall_SiebelLinux7.3`

Note: The `<FolderNameOfComponent>` is the folder name of each component where the respective component files reside.

2. At the command prompt, type the following command: `<uninstallscriptname> -silent`.

Note: The `<uninstallscriptname>` is the uninstaller script.

For example:

Operating System	Command
Windows	`uninstall7.3.4.bat -silent`
Solaris and AIX	`./uninstall7.3.4.sh -silent`

Linux	`IC Side: ./Uninstall_AICLinux7.3`
	` -i silent`
	
	`Siebel Side: ./Uninstall_SiebelLinux7.3`
	`-i silent`

3. Press **Enter**.

Note: After the uninstallation is complete, sometimes the uninstall program does not delete the 7.3.x. The x is the SP number for which the uninstall program is executed. In such a case, you need to manually delete the 7.3.x subfolder from the `.../IC73/ICServicePacks` folder.

Chapter 6: Updating IC help

The IC help in HTML format is integrated with the IC application. When you install IC on a system, the installer updates the help files only for Avaya Agent and Avaya Agent Web Client components. For other IC components, the installer provides the `help.zip` file containing the required HTML help files. You must manually extract these help files on the respective IC systems.

Note: For the latest `help.zip` file go to the Avaya support site at http://support.avaya.com. The help.zip file on the Avaya support site will be regularly updated for any major changes in the help. For more information, see Updating the IC help by downloading the help.zip from the Avaya support site.

This section provides the procedures to update the help files for various IC components installed on Windows, Solaris and AIX operating systems.

The `help.zip` file contains the help files for the following IC components:

- Business Advocate

- Template Manager (RL Manager)

- Webservice

- Config Accelerator (CA)

- Database Designer

- IC Manager

- Report Wizard

- Workflow Designer

On the Solaris system you must update the help files for the following IC components:

- Template Manager (RL Manager)

Note: For all the above mentioned components, you must update the help files at the location where you installed these components.

In the IC installer you can find the following packages that contain the changed help.zip files:

- IC734WinServer.zip

  This package contains the changed help files for the following IC server components:

  - Business advocate

  - Templatemanager

- ▪ Webservices

- IC734WinAdmin.zip

  This package contains the changed help files for IC Admin components:

  - ▪ Config accelerator (CA)

  - ▪ Database designer

  - ▪ IC Manager

  - ▪ Report Wizard

  - ▪ Workflowdesigner

- IC734SolServer.zip

  This package contains the changed help files for the following IC server components:

  - ▪ Templatemanager

  - ▪ webservices.html

- IC732AixServer.zip

  This package contains the changed help files for the following IC server components:

  - ▪ Templatemanager

  - ▪ webservices.html

Updating help for IC Admin components

Installed on Windows platform

1. On the system where you have installed IC Admin components, go to the `IC_INSTALL_HOME\IC73\`help folder.

2. (Optional) Backup all files and folders from the help folder.

3. (Optional) From the IC installer, extract the IC734WinAdmin package.

4. From the extracted IC734Admin folder, open the help.zip file.

5. From the `help.zip` file, extract the help folder to the `IC_INSTALL_HOME\IC73\` folder on the system where you installed the IC Admin components.

Updating help for IC server components

Installed on Windows platform

1. On the system where you have installed IC server components, go to the `IC_INSTALL_HOME\IC73\help` folder.

2. (Optional) Backup all files and folders from the help folder.

3. From the IC installer, extract the IC734WinServer package.

4. From the extracted IC734WinServer folder, open the help.zip file.

5. From the `help.zip` file, extract help folder to the `IC_INSTALL_HOME\IC73\` folder.

Installed on Solaris platform

1. On the Solaris server where you have installed IC server components, go to the `IC_INSTALL_HOME\IC73\help` folder.

2. (Optional) Backup all files and folders from the help folder.

3. From the IC installer, extract the IC734SolServer package.

4. From the extracted IC734SolServer folder, open the `help.zip` file.

5. In the `help.zip` file, open the help folder.

6. From the help folder, extract the templatemgrhelp folder and the webservices.html file to the `IC_INSTALL_HOME\IC73\help` folder.

Installed on AIX platform

1. On the AIX server where you have installed IC server components, go to the `IC_INSTALL_HOME\IC73\help` folder.

2. (Optional) Backup all files and folders from the help folder.

3. From the IC installer, extract the IC732AIXServer package.

4. From the extracted IC732AIXServer folder, open the `help.zip` file.

5. In the help.zip file, open the help folder.

6. From the help folder, extract the templatemgrhelp folder and the webservices.html file to the `IC_INSTALL_HOME\IC73\help` folder.

Updating the IC help by downloading the help.zip from the Avaya support site

1. Download the help.zip file from the Avaya support site: http://support.avaya.com.

2. Extract the help.zip file as explained in the following table:

Components	Operating System	Location where to update the help	Files and Folders that needs to be updated
Admin	Windows	`IC_INSTALL_HOME\IC73\help`	CA Database designer IC Manager Report Wizard Workflowdesigner
Server	Windows	`IC_INSTALL_HOME\IC73\help`	Business advocate Templatemanager Webservices
	Solaris and AIX	`IC_INSTALL_HOME\IC73\help`	Templatemanager webservices.html

Comments on this document? infodev@avaya.com

Chapter 7: Technical Support

If you experience trouble with IC 7.3.4, you must:

1. Retry the action. Carefully follow the instructions in written or online documentation.

2. Check the documentation that was provided with your hardware for maintenance or hardware-related problems.

3. Note the sequence of events that led to the problem and the exact messages displayed. Have the Avaya documentation available.

4. If you continue to experience problem, contact Avaya Technical Support by one of the following ways:

   ▪ Logging in to the Avaya Technical Support Web site http://support.avaya.com/.

   ▪ Calling or faxing Avaya Technical Support at one of the telephone numbers in the Avaya Support Dashboard listings on the Avaya support Web site.

You might be asked to email one or more files to Technical Support for analysis of your application and the environment.

Note: If you have difficulty reaching Avaya Technical Support through the above URL or email address, visit the http://www.avaya.com for further information.

Avaya Global Services Escalation Management provides the means to escalate urgent service issues. For more information, see the Escalation Contacts listings on the Avaya Web site.

For information about patches and product updates, see the Avaya Technical Support Web site http://support.avaya.com/.

Chapter 8: Feature Pack files list

For information on the time stamp and version number of various service pack files for Avaya Interaction Center 7.3.x, see the Service Pack file list with modification time stamp and version numbers for Avaya Interaction Center 7.3.x document on the Avaya Support site: http://support.avaya.com/.

Comments on this document? infodev@avaya.com

Chapter 9: Customer found defects, known issues and workarounds, troubleshooting

For information on known issues and troubleshooting included in Avaya Interaction Center 7.3.4 release, see the List of Fixed Issues, Known Issues, and Troubleshooting for Avaya IC 7.3.x. document on the Avaya Support site: http://support.avaya.com/

Chapter 10: Avaya Technical Support contact information

You can contact Avaya Interaction Center Technical Support through Internet, e-mail, or telephone. To contact Avaya Interaction Center support please visit https://support.avaya.com/contact/.