Avaya Interaction Center 7.3.10 Service Pack Release Notes

Release 7.3.10

August 2021

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“**Hosted Service**” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDERTHE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “**Software**” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “**Designated Processor**” means a single stand-alone computing device. “**Server**” means a Designated Processor 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

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "**Unit**" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

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 only 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

You acknowledge and agree that it is Your responsibility 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, its licensors, its suppliers, 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: https://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 7.3.10 Service Pack (SP) Release Notes provides information on installation and configuration of IC 7.3.10 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 7.3.10 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 7.3.10 Service Pack.

The audience for this guide includes:

- Application consultants
- Integration consultants
- Avaya Business Partners
- Customers

Documents changed in IC 7.3.10 Service Pack

The following files are updated in IC 7.3.10 Service Pack Release:

- Avaya Interaction Center List of Fixed Issues, Known Issues, and Troubleshooting 7.3.x
- Avaya Interaction Center and Avaya Operational Analyst Overview and Specification
- IC Installation Planning and Prerequisites
- IC Installation and Configuration
- IC Administration Guide
- IC Alarms User Guide

- IC Security Guide
- IC Agent User Guide
- File list with modification time stamp and version numbers for AIC 7.3.x

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.

Title	Description
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 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.
Avaya IC for Siebel Integration Guide	The Avaya Interaction Center for Siebel integration combines Avaya Interaction Center (IC). Release 7.3.x with the Siebel applications. The integration of Avaya IC with Siebel facilitates you to use the customer management features in the Siebel software and the features in Avaya IC that automate the processing of customer contacts.
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	

Title	Description
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 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

Title	Description
	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.

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

Course code	Course title
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, click the product name and select 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) 7.3.10 Service Pack (SP) is the tenth release on top of IC 7.3. The SP is a cumulative release which also includes all the fixes from IC 7.3.1 SP, IC 7.3.2 FP, IC 7.3.3 FP, IC 7.3.4 SP, IC 7.3.5 FP, IC 7.3.6 SP, IC 7.3.7 SP, IC 7.3.9 SP, and IC 7.3.10 SP. 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 7.3.10 SP level to ensure you have a complete set of fixes. IC 7.3.10 SP does not include a redelivery of the entire IC product. The IC 7.3.10 SP can be directly installed on IC 7.3. Follow the instructions in the Release Notes when installing and configuring the IC 7.3.10 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 “Service 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, 7.3.4, 7.3.5, 7.3.6, 7.3.7, 7.3.8, 7.3.9 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.

Note: Solaris OS is not supported since Interaction Center 7.3.9. All the information related to Solaris is only applicable to Interaction Center Release till 7.3.8 inclusively.

Note: The packages for Siebel Part on Linux OS are not provided with 7.3.10 Release. These packages will be released separately soon.

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 7.3.10 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 Integration Guide

Web browsers tested in IC 7.3.10 Service Pack

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

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

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	✓	✓	✓	✓	✓

Channel / Feature	**Functionality Supported**	**Avaya Rich Client**	**Avaya Web Client**	**Avaya SDK Client**	**Avaya Siebel Native Client**	**Avaya Siebel Hybrid Client**
	Transfer to Virtual Queue	✓	✓	✓	✓*	✘
	Switch to caller	✓	✓	✓	✘	✘
	Transfer to Agent	✓	✓	✓	✓	✓
Email	Reply / Reply All	✓	✓	✓	✓	✓
	Forward	✓	✓	✓	✓	✓
	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	✓	✓	✓	✘	✓
	Blind Transfer to Queue	✓	✘	✘	✘	✘
	Use local/global resource for responses	✓	✓	✘	✘	✘
	Wrap	✓	✓	✓	✘	✓

Channel / Feature	Functionality Supported	Avaya Rich Client	Avaya Web Client	Avaya SDK Client	Avaya Siebel Native Client	Avaya Siebel Hybrid Client
	Emoticons	✓	✓	✓	✘	✓
	Chat Typing status	✓	✓	✓	✘	✓
	Join Us	✓	✓	✓	✘	✓
	Transfer to Virtual Queue	✓	✓	✓	✘	✓
Contact History	View	✓	✓	✓	✘	✘
	Filter	✓	✓	✓	✘	✘
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 website, http://support.avaya.com.
You can download the latest patches and installation instructions.

Platform updates in 7.3.10 SP

Support for the following platforms was added in 7.3.10 SP:

Internal Products:

- Web LM 8.1.3

3rd Party Products:

- Java 8.0.292 – Open JDK
- Tomcat 10.0.4
- OpenSSL 1.1.1 (TLS 1.3 Support)
- Siebel Innovation Pack 21.5

Behavioral Changes

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

Change in SSL communication (Introduced in IC 7.3.10 FP)

- OpenSSL library version is upgraded to 1.1.x
- Directory Server (DS) and HTTPConnector Server are modified from IC 7.3.10 FP onwards to accept TLSv1.3 during TLS handshake.
- Alarm Server is modified from IC 7.3.10 FP onwards to support AES256 encryption.
- **TLSProtocol:**

  Valid Values:
  1) **TLS 1.0**
  2) **TLS 1.1**
  3) **TLS 1.2**
  4) **TLS 1.3**

  Default Value : TLS 1.2

  - **CipherList:**

  Valid Values :

  1) ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2:-SSLv3
  2) ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2

  Default Value:
  ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2:-SSLv3

To set the above parameters:

a. Log in to IC Manager with Admin privileges.

b. Edit the **DS/HTTPConnector** server

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

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

e. Provide the values for this new couple as:

Name	Value
TLSProtocol	TLS 1.0
CipherList	`ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2`

f. Click **OK**.

g. Click **OK** in DS/HTTPConnector Editor.

h. Restart the **DS/HTTPConnector** in IC Manager.

i. Repeat the above steps for all DS/ HTTPConnector servers configured in the IC system.

SSL protocol compatibility in IC

IC Client	IC Server	TLS Protocol	CipherList
IC 7.3.3	IC 7.3.5	TLS 1.0	`ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2`
IC 7.3.4	IC 7.3.5	TLS 1.0	`ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2`
IC 7.3.5	IC 7.3.5	TLS 1.0/TLS 1.1	`ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2`
IC 7.3.5	IC 7.3.5	TLS 1.2	`ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2:-SSLv3`
IC 7.3.10	IC 7.3.10	TLS 1.3	`ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2:-SSLv3`

Note:

- At least one IC Manager system should be upgraded to release 7.3.10.
- The properties **TLSProtocol** and **CipherList** must be removed when ALL the clients are upgraded to IC 7.3.10.
- Configuration parameter **allow_sslv3** is obsolete, and has to be removed when IC is upgraded to 7.3.10.

Tiny MCE HTML editor (Introduced in IC 7.3.9 SP)

Email HTML editor has been replaced in Avaya Agent Rich client in 7.3.9 release. 3rd party Ephox EditLive library has been replaced with Tiny MCE for Swing 5.4.2.
The transition from Ephox to Tiny MCE is seamless and does not require any actions from an agent.
The most of Ephox properties will be converted to TinyMCE properties automatically. However some properties are not present in TinyMCE, so they are not translated.

The following Ephox settings are translated to Tiny MCE:

- Default style
- Autolink plugin
- Fonts
- Font sizes
- Lists
- Bold/Italic/Underline
- Text color
- Background color
- Insert image
- Insert hyperlink
- Predefined links
- Predefined e-mails
-

The following Ephox settings are not translated to Tiny MCE:

- WysiwygEditor
- HtmlFilter
- PlacesInDocument

See details in the following documents: Avaya Interaction Center Agent User Guide, **Avaya Interaction Center Installation and Configuration, Avaya Interaction Center Administration Guide.**

Open JDK (Introduced in IC 7.3.9 SP)

Open JDK (Introduced in IC 7.3.9 SP)

Since IC 7.3.9 Release Oracle Java has been replaced with Open JDK Zulu Java for IC Server components. New Java binaries will be provided to Avaya folder during the Service Pack installation. Client applet-based applications such as AAWC still use Oracle Java.

Cobrowse Feature removal (Introduced in IC 7.3.9 SP)

Cobrowse feature for Website chat and AARC has been removed since IC 7.3.9 Release. “Please wait” dialog for new chats has been removed from AARC as well.

Microsoft Visual C++ Redistributable Package 2017 (Introduced in IC 7.3.9 SP)

All IC components based on C++ code have been recompiled using Microsoft Visual C++ 2017. So Microsoft Visual C++ Redistributable Package 2017 needs to be installed on each machine with IC components. This package will be installed during IC 7.3.9 Release installation.

Licensing changes due to WebLM Upgrade from 6.3.4 to 7.0.1 version (Introduced in IC 7.3.8 SP)

After upgrade WebLM from 6.3.4 to 7.0.1 version, HostID will be changed. So after AIC upgrade to 7.3.8 SP WebLM would not work. You have to request a replacement license file for it.

This request is described in “AIC Installation Planning and Prerequisites guide” document, chapter 8:”Interaction Center Licensing”, section “Requesting a replacement license file”, https://downloads.avaya.com/css/P8/documents/100159305

Poller/ICEmail Server behavior for RFC compliant email addresses (Introduced in IC 7.3.5 FP)

In IC 7.3.5 release, we have optimized the way Poller Server checks for RFC compliance for "From", "Sender" & "Reply-To" headers of an incoming email. From IC 7.3.5 release onwards, the system would verify if an incoming email contains at least one RFC compliant header in the “From" or "Sender" or "Reply-To" header fields. Even if one of these fields is valid, the email will be processed. To make things simpler, “Allow Only RFC Compliant Emails to be processed” configuration field from “Poller” tab of Poller server has been removed.

Refer IC Administration Guide for Poller server configuration details.

Failed Login Notification (Introduced in IC 7.3.5 FP)

IC 7.3.5 feature pack failed login attempts are monitored and an alarm is raised. For more details refer to Section Failed Login Notification in **Enhancements in IC 7.3.5 Feature Pack**

Change in SSL communication (Introduced in IC 7.3.5 FP)

- OpenSSL library version is upgraded to 1.0.x
- Directory Server (DS) and HTTPConnector Server are modified from IC 7.3.5 FP onwards to accept TLSv1.1 and TLSv1.2 during TLS handshake.
- IC SSL/TLS clients use TLSv1.2 during TLS handshake by default.

  Note:

  A client from an older version of IC (IC 7.3.3 and IC 7.3.4) cannot communicate with an upgraded IC 7.3.5 Directory Server for 'Login' or 'Authenticate' requests. To enable communication during upgrade scenarios, use the following configuration parameters. These configurations help in overriding the default values. IC Clients releases prior to 7.3.3 FP will not work with IC release 7.3.5.

- **TLSProtocol:**

  Valid Values:
  5) **TLS 1.0**
  6) **TLS 1.1**
  7) **TLS 1.2**
  Default Value : TLS 1.2

- **CipherList:**

  Valid Values :
  3) ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2:-SSLv3
  4) ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2

  Default Value:
  ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2:-SSLv3

To set the above parameters:

j. Log in to IC Manager with Admin privileges.
k. Edit the **DS/HTTPConnector** server
l. Go to the **Configuration** tab.
m. Click **New** to open the 'CTI Type Editor'.
n. Provide the values for this new couple as:

Name	**Value**
TLSProtocol	TLS 1.0
CipherList	`ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2`

o. Click **OK**.

p. Click **OK** in DS/HTTPConnector Editor.

q. Restart the **DS/HTTPConnector** in IC Manager.

r. Repeat the above steps for all DS/ HTTPConnector servers configured in the IC system.

SSL protocol compatibility in IC

IC Client	IC Server	TLS Protocol	CipherList
IC 7.3.3	IC 7.3.5	TLS 1.0	`ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2`
IC 7.3.4	IC 7.3.5	TLS 1.0	`ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2`
IC 7.3.5	IC 7.3.5	TLS 1.0/TLS 1.1	`ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2`
IC 7.3.5	IC 7.3.5	TLS 1.2	`ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2:-SSLv3`

Note:

- At least one IC Manager system should be upgraded to release 7.3.5.
- The properties **TLSProtocol** and **CipherList** must be removed when ALL the clients are upgraded to IC 7.3.5.
- Configuration parameter **allow_sslv3** is obsolete, and has to be removed when IC is upgraded to 7.3.5.
- If you are using Avaya IC-Siebel Integration on AIX platform with IC Release 7.3.2 then you must install **`IC732AixServer_Openssl1.xUpgrade_patch.tar`** on IC Release 7.3.2 AIX Server. Installing the patch will enable IC Release 7.3.5 (IC Server or clients) to communicate with Avaya Communication Driver (AICD)on AIX Siebel Server.

Change in ASGPlugin to support new ASG Keys Update (Introduced in IC 7.3.5 FP)

Access Security Gateway keys update. In keeping with NIST guidelines and industry best practices, Avaya is rotating the security keys associated with remote maintenance access through the Access Security Gateway (ASG).

ASGPlugin is used for remote access. To perform configuration changes after IC 7.3.5 installation, refer the ASGPlugin Keys Update for Remote Access section below.

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. Log in 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. Hang up 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 an agent is in Automatic blending mode, the 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 7.3.10 Service Pack

OAuth 2.0 Support

Since 7.3.10 Release IC supports OAuth 2.0. IC email account authorization uses OAuth2 to communicate with Microsoft Exchange Online accounts. Any other cloud services that use OAuth2 for authorization are not supported.

Requirements

IC’s core & DnA hosts must have access to the Azure cloud.

Known limitations

No known limitations. Cloud accounts are subject to the same rules within IC as regular accounts. Refer to IC documentation for details.

Configuration

Azure side
Using admin account create new MS Graph application.
It is necessary to add http://localhost to the Redirect URIs list.

AIC side

At core host:

Note: Make sure IC Email server & Poller servers are stopped during certificate installation.

Install Office365 certificates (base64 format, containing full chains) into %AVAYA_IC73_HOME%\etc. So here will present smtp.office365.com.pem and outlook.office365.com.pem files, one per outgoing and incoming. Typically, they are identical.

Note: %AVAYA_IC73_HOME%\Java\bin\server is automatically added at the beginning of the “path” system variable after applying the IC 7.3.10.

At DnA host:
Upgrade database with new design\CallCenterQ\ccq.adl and design\repository\repository.adl definitions.

Use the provided files or edit existing ones to make the following changes:

<table>
<tr><th>Database type</th><th>Changes</th></tr>
<tr><td>MSSQL</td><td>

```
@@ -6590,11 +6590,11 @@ DEFINE TABLE qem_mailaccount WITH DATASOURCE
CallCenterQ
             ENUM "POP","IMAP"
             DESC = "email account type ( POP or IMAP)"
             DEFAULT = "POP";
       "authtype" LABEL "Authtype"
             LOCKED
-            ENUM "NTLM","APOP","MD5"
+            ENUM "NTLM","APOP","MD5","XOAUTH2"
             DESC = "authentication type"
             DEFAULT = "NTLM";
       "enabletls" LABEL "Enable TLS"
             LOCKED
             INTEGER MAX "1" MIN "0"
@@ -6695,13 +6695,33 @@ DEFINE TABLE qem_mailaccount WITH DATASOURCE
CallCenterQ
             LOCKED
             VSTRING OF LENGTH 1
             DESC = "If set, the email server must log into the mail
server using secure passwords";
       "smtpauthtype" LABEL "SMTP Authtype"
             LOCKED
-            ENUM "PLAIN","NTLM","CRAMMD5","LOGIN"
+            ENUM "PLAIN","NTLM","CRAMMD5","LOGIN","XOAUTH2"
             DESC = "smtp authentication type"
             DEFAULT = "PLAIN";
+      "oauthcid" LABEL "OAuth client ID"
+            LOCKED
+            VSTRING OF LENGTH 38
+            DESC = "OAuth client ID";
+      "oauthauthority" LABEL "OAuth authority"
+            LOCKED
+            VSTRING OF LENGTH 255
+            DESC = "OAuth authority";
+      "oauthscopes" LABEL "OAuth scopes"
+            LOCKED
+            VSTRING OF LENGTH 1000
+            DESC = "OAuth scopes";
+      "oauthruri" LABEL "OAuth redirect uri"
+            LOCKED
+            VSTRING OF LENGTH 1000
+            DESC = "OAuth redirect uri";
+      "oauthdata" LABEL "OAuth data cache"
+            LOCKED
+            TEXT
+            DESC = "OAuth data cache";
 };
```

</td></tr>
</table>

Oracle

```
@@ -6590,11 +6590,11 @@ DEFINE TABLE qem_mailaccount WITH DATASOURCE
CallCenterQ
              ENUM "POP","IMAP"
              DESC = "email account type ( POP or IMAP)"
              DEFAULT = "POP";
       "authtype" LABEL "Authtype"
              LOCKED
-             ENUM "NTLM","APOP","MD5"
+             ENUM "NTLM","APOP","MD5","XOAUTH2"
              DESC = "authentication type"
              DEFAULT = "NTLM";
       "enabletls" LABEL "Enable TLS"
              LOCKED
              INTEGER MAX "1" MIN "0"
@@ -6695,13 +6695,33 @@ DEFINE TABLE qem_mailaccount WITH DATASOURCE
CallCenterQ
              LOCKED
              VSTRING OF LENGTH 1
              DESC = "If set, the email server must log into the mail
server using secure passwords";
       "smtpauthtype" LABEL "SMTP Authtype"
              LOCKED
-             ENUM "PLAIN","NTLM","CRAMMD5","LOGIN"
+             ENUM "PLAIN","NTLM","CRAMMD5","LOGIN","XOAUTH2"
              DESC = "smtp authentication type"
              DEFAULT = "PLAIN";
+      "oauthcid" LABEL "OAuth client ID"
+             LOCKED
+             VSTRING OF LENGTH 38
+             DESC = "OAuth client ID";
+      "oauthauthority" LABEL "OAuth authority"
+             LOCKED
+             VSTRING OF LENGTH 255
+             DESC = "OAuth authority";
+      "oauthscopes" LABEL "OAuth scopes"
+             LOCKED
+             VSTRING OF LENGTH 1000
+             DESC = "OAuth scopes";
+      "oauthruri" LABEL "OAuth redirect uri"
+             LOCKED
+             VSTRING OF LENGTH 1000
+             DESC = "OAuth redirect uri";
+      "oauthdata" LABEL "OAuth data cache"
+             LOCKED
+             VSTRING OF LENGTH 9999
+             DESC = "OAuth data cache";
 };
```

Upgrade database using Database Designer.
Refer to the Microsoft manuals for information about configuring outgoing & incoming servers.

IC Email Accounts

Configure email account in ICManager. The following parameters were added:

Tab	Field	Description
Outgoing Email Server tab	Use SMTP Authentication	Select this option to enable SMTP AUTH. If this option is selected, you can view the following options: ● Logon account: Provide the login detail for SMTP AUTH. ● Password: Provide the password for SMTP AUTH (is not required when the XOAUTH2 authentication type is used). ● Confirm Password: Re-enter the Password (is not required when the XOAUTH2 authentication type is used). ● Use Secure Authentication: Select this option to send SMTP AUTH info securely. ● Authentication Type: This option is enabled if you select Use Secure Authentication option. The available options under Authentication Type are: - LOGIN - NTLM - CRAMMD5 - XOAUTH2
Incoming Email Server tab	Password / Confirm	Enter the password for the email account in both fields (is not required when the XOAUTH2 authentication type is used).
	Authentication Type	Select NTLM, MD5 or XOAUTH2 as authentication types for this email account. For more information, see Configuring the email accounts for SSL on page 363.
OAuth tab	Client ID	Enter Client ID of the registered Azure application.
	Authority	Enter common part of an authority url in form https://login.microsoftonline.com/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
	Redirect URI	Enter Redirect URI of application. At the moment it has to be http://localhost
	Scopes	Enter scopes for the registered Azure application divided by semicolon. Typically, offline_access; https://outlook.office.com/IMAP.AccessAsUser.All; https://outlook.office.com/POP.AccessAsUser.All; https://outlook.office.com/SMTP.Send

Restart the core services machine to apply the changes above.

References

- Avaya Interaction Center Installation and Configuration on Microsoft Windows/Oracle Solaris/IBM AIX, Chapter 12: Configuring Email Management

- https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app
- https://docs.microsoft.com/en-us/exchange/client-developer/legacy-protocols/how-to-authenticate-an-imap-pop-smtp-application-by-using-oauth
- https://support.microsoft.com/en-us/office/pop-imap-and-stmp-settings-8361e398-8af4-4e97-b147-6c6c4ac95353
- https://docs.microsoft.com/en-us/microsoft-365/enterprise/plan-for-third-party-ssl-certificates?view=o365-worldwide

Enhancements in IC 7.3.9 Service Pack

SNMP v3 Support

Support of SNMP v3 protocol for IC Alarm server has been introduced in 7.3.9 release. The previous protocol version is still supported. Customer can continue using SNMP v2 or configure SNMP v3. See details in the following documents: Avaya Interaction Center Alarms User Guide, Avaya Interaction Center Core Services Programmer Guide, Avaya Interaction Center Administration Guide.

CSPortal Enhanced logging

Logging mechanism for IC CSPortal has been improved. New CSPortall logging feature uses log4j2 library. It is configured by changing file **log4j2.properies**. It can be found in %AVAYA_IC73_HOME%\comp\csportal\WEB-INF\classes\ folder.

By defaut CSPortal logs are written to %AVAYA_IC73_HOME%\logs\CSPortal.log.

Each class of CSPortal has its own logger, which allows detailed logging control. To change overall logging level root logger level should be changed.

rootLogger.level = error

If only one or few loggers are desired to have different logging level, it is possible to specify it's level in config file:

```
logger.rolling.name = com.example.my.app
logger.rolling.level = debug
rootLogger.level = error
rootLogger.appenderRef.stdout.ref = RollingFile
```

Size of roll-over file can be set by

appender.rolling.policies.size.size=1MB

Name of roll-over files can be set by

```
property.filename = ../logs/CSPortal.log
appender.rolling.filePattern = ../logs/CSPortal-%i.log
```

The first line sets current file name. The second line configures rolling file name pattern.
By defaut data is logged into %AVAYA_IC73_HOME%/logs/CSPortal.log file.

For details visit https://logging.apache.org/log4j/2.x/manual/configuration.html

To change logging layout:
%d – Outputs the date of the logging event. The date conversion specifier may be followed by a set of braces containing a date and time pattern string per per SimpleDateFormat. Default - 2012-11-02 14:34:02,123
%p – Outputs the level of the logging event.
%c – Outputs the name of the logger that published the logging event. The logger conversion specifier can be optionally followed by precision specifier, which consists of a decimal integer, or a pattern starting with a decimal integer.
%M – Outputs the method name where the logging request was issued.
%t – Outputs the name of the thread that generated the logging event.
%m – Outputs the application supplied message associated with the logging event.

For details visit https://logging.apache.org/log4j/2.x/manual/layouts.html

Inter-domain Single-Step Conference scenario improvement

Now in case of SSC between agents from different domains, it is possible to utilize the single VDUID. When the target TS (monitoring the supervisor) gets a SSC call from an agent (monitored by other TS), it retrieves the UCID of the call from the C_CONNECTED event and tries to find the existing VDUID using this UCID. The new option was implemented in TS - find_vdu_by_ucid_ssc. To enable the new feature, it is required to set this parameter to true for the TSes via the IC Manager (double- click the TS server and navigate to the Configuration tab) and restart the TS servers.

Switch to Caller and Logout in Wrapup features for Siebel

The Logout In Wrapup feature allows agents to log out while they have work items in wrapup state. In this case, the wrapup will be completed automatically prior to logout.

The Switch to Caller/Destination feature can be used during a consultation call, when an agent, which handles a call from a customer, needs assistance from other agent. This feature lets the agent switch between talking to the other agent and talking to the caller (the customer).

See Avaya IC for Siebel Integration Guide document for details.

Enhancements in IC 7.3.6 Service Pack

Default Pool Outbound Email Selection

From Release 7.3.6, an administrator can configure the **FilterPoolsByTenant** property to restrict an agent's view to only the pools of the tenant associated with the agent's primary workgroup.

A new property **FilterPoolsByTenant** is added to **Agent/Desktop/Email** property section in IC Manager with the following values:

- Yes – agents can see only the pools associated with the tenant for the primary workgroup.
- No – agents can see all the pools. This is the default value.

In case of any changes to this property or pools in IC Manager it is necessary to re-login to AARC. To enable this functionality it is required to perform steps mentioned in the "Import Seed Data" section for 7.3.6 SP.

Enhancements in IC 7.3.5 Feature Pack

Publish EDU Field {ucid} to Siebel in AIC-Siebel Integration

In IC-Siebel integration, EDU field ***{ucid} – Universal Call Identifier –*** will be pushed to Siebel as a common EDU field through the IC telephony events ***OnCallIncoming***, ***OnNewWorkItem***, and ***OnCallConnect.*** The Siebel event handler then captures {ucid} field for further processing. With this change *{ucid}* becomes a common EDU field for the aforementioned events and there is no need to add this field explicitly in the configuration file ***AICDStrings.txt***.

In addition, a provision is made for ***OnCallConnect*** event to push additional EDU fields through configuration file ***AICDStrings.txt***.

For more information on AICD events & parameters, see Avaya IC 7.3.x for Siebel Integration Guide on the Avaya Support.

Chat Pop-out/Pop-in and tabbed chat

Prior to IC 7.3.5, AARC webagent could only display one chat contact at a time. Each time an agent activated a chat, the chat would open in the webagent window replacing the last activated contact. From IC 7.3.5 onwards, for each incoming chat a tab is added in the webagent window. With this feature, the agent shall be able to view all chats in the web agent simultaneously in the form of different tabs. On activating a chat from the chatlist, the corresponding tab in the webagent would be brought to focus. Similarly, if a specific tab is selected in the webagent, the corresponding chat gets selected in the chatlist. A chat contact tab can only be closed if the chat has been completed. The agent can continue using the existing features such as the webagent toolbar, the contact menu and the resources for each of the chat tabs.

The agent also has the flexibility to pop-out or open any of the chats in a separate window, as opposed to in a tab, by either using the shortcut key combination of Control+Shift+W or by clicking on ↗ icon in the webagent toolbar. Similar to the chat contact tabs, if any of these popped-out windows is brought to focus, the corresponding chat gets activated and selected in the chatlist. The agent can use the webagent toolbar to manage the chat in the popped out window. However the **Contact** menu and the resource panel are not available while the chat is popped out. The agent can merge back or pop-in the chat window back in thewebagent window by either using the short cut key combination of Control+Shift+P or by clicking on ↙ icon in the popped out window toolbar . Popping-in the chat will cause the chat contact to appear as a tab in the webagent window.

By default the size of Popped Out window will be calculated based on the screen dimension, however it can be customized. The **height** and the **width** values (in pixel) for the property SeparateChatWindow in AgentPreferences.xml has to be modified.

Example:

<SeparateChatWindow closeOperation="1" height="600" width="600" />

The values cannot be bigger than the screen dimension or lesser than the minimum size of the chat panels. If the values are incorrect, the application calculated default dimensions would be used

To customize the size of the popped-out window, use the below steps:

1) On an AARC machine, login an agent. Navigate to <AVAYA_IC_HOME>\Webagent\agents\<agent_id>
2) After backing up the AgentPrefrences.xml file, add <SeparateChatWindow closeOperation="X" height="Y" width="Z" /> to the file and save it.
   Where X can have one of the below values:

Value	Meaning
1	The default option (do nothing). If the agent clicks on the cross button, no action will be taken, if the chat is not yet completed.
2	The popped out window is merged back to the webagent window as a tab.
3	Close the popped out window, but keep the task in the chat list. This operation ensures that the chat session is intact, even though the popped out window is closed. If the agent activates the chat again using the task list, the chat will appear in a tab in the web agent.

   Where Y would contain the value in pixels
   Example: height="600"
   Where Z would contain the value in pixels
   Example: width="600"
3) Place this file in <AVAYA_IC_HOME>\Webagent\agents\<agent_id> folder on each agent machine.

Enhanced Chat Notification

To allow agents to do other tasks while waiting for a customer's response to a chat contact, rich client now provides the below notifications:

Visual Notifications:
Visual notifications can be of two types:

1) Flashing of web-agent icon and chat contact tab

2) SLA Notification

1) Flashing of Web Agent icon and chat contact tab:

If web agent is not in focus, to notify the agent that the customer has responded to a chat contact, the web agent icon in the task bar flashes thrice and then converts to solid orange till the web agent is brought in focus. If web agent was already in focus when the customer responded, with the agent working on a different contact, the web agent icon will only flash thrice. The tab corresponding to the chat contact for which the message has been received, also flashes thrice and then solidifies till the tab is brought in focus. The number of times and the rate at which the chat contact tab in the web agent window flashes, can be customized by following the steps below:

1. On an AARC machine, login an agent. Navigate to <AVAYA_IC_HOME>\Webagent\agents\<agent_id>
2. Backup the file AgentPrefrences.xml file.
3. After backing up the AgentPrefrences.xml file. Add <Alarming flashes_number="x" interval="y" /> to the file and save it. Where x is the number of times the tab should flash before it solidifies and y is the interval in milliseconds. The default value is <Alarming flashes_number="3" interval="800" />
4. Place this file in <AVAYA_IC_HOME>\Webagent\agents\<agent_id> folder on each agent machine.

2)SLA Notification:

The Admin can define 3 SLAs within which the agent should respond back to the customer for chat contacts. If the customer has responded to a chat contact and the web agent is either not in focus or the agent is working on a different contact in the web agent, the corresponding chat in the chat list is color coded to notify the agent of the response. The color coding is achieved by changing the background and font color of the chat in the chatlist. The chat remains color coded till the agent views the corresponding chat in web agent. After the agent views the chat, the color coding is reset.

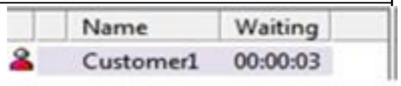
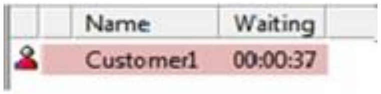
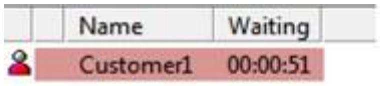
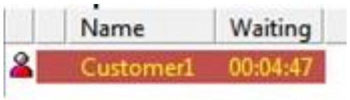
Further, each time the ‘wait-time’ of a chat contact exceeds one of the SLAs defined by the Admin, the corresponding chat in the chatlist is color coded to notify the agent. Once the agent responds back to the customer, the color coding is reset.

The SLA timings, background and font colors used for each of the above mentioned color coding are customizable and can be changed using the below mentioned steps:

1. Go to IC manager. Navigate to Property Declarations.
2. Under Agent/Desktop/Chat/Application, add the below properties:

Property Name	Property type
SLATimings	String
ChatListBGandTextColors	String
EnableChatListColorCoding	Boolean

3. Navigate to Tools-> Groups->Properties.
4. Under Agent/Desktop/Chat/Application, add the below properties.

<table>
<tr><th>Property Name</th><th>Default value of property</th><th>Meaning</th></tr>
<tr><td><b>SLATimings</b></td><td>20,40,60</td><td>Specifies the three SLAs. The values specified should be in seconds and separated by commas.</td></tr>
<tr><td><b>ChatListBGandTextColors</b></td><td>E4DFEC,E6B9B8,D99694 ,C0504D,000000,000000,000000 ,FFFF00
Here 'E4DFEC,E6B9B8,D99694,C0504D,000000,000000,000000,FFFF00' is the list of colors
(Hex equivalents for RGB values) to be used for chatlist color coding. The first four hex values correspond to the background colors, the last four colors correspond to the text colors to be used for each of these background colors.</td><td>Below is the table, mapping the background & text colors and sample screen shots of how the out of box colors would appear. The hexa-equivalents of RGB should not be preceded by ‘0x’ and is case insensitive. If the value of this property is erroneous, the default values are used.
<table>
<tr><th>Background color</th><th>Text Color</th><th>Sample Screen shot from Rich Client</th></tr>
<tr><td>E4DFEC</td><td>000000</td><td>
Name Waiting
Customer1 00:00:03</td></tr>
<tr><td>E6B9B8</td><td>000000</td><td>
Name Waiting
Customer1 00:00:37</td></tr>
<tr><td>D99694</td><td>000000</td><td>
Name Waiting
Customer1 00:00:51</td></tr>
<tr><td>C0504D</td><td>FFFF00</td><td>
Name Waiting
Customer1 00:04:47</td></tr>
</table></td></tr>
<tr><td><b>EnableChatListColorCoding</b></td><td>Yes</td><td>Enables the color coding feature. Setting this to ‘No’ would disable the color coding</td></tr>
</table>

Audio notification:

If web agent is not in focus or the agent is working on a different contact in web agent, the agent will be notified by a sound to indicate that the customer has responded to the chat.

Below are the configurations to enable audio notifications:

1. In AARC , in the Webagent go to Tools->preferences. In preferences select the **Contact** tab. Enable **Alert with sound when a new contact Arrives**.
2. In Application.properties file (Path: <AVAYA_IC_73_HOME\Webagent>), add the below:
   a) **webagent.sounds.enabled**=true
   b) **sounds.oncustomeralert.enabled**=true
   c) **mediaspecific.sounds.onarrival** = true

Customizing sound alerts

1) For customizing the sound alerts to indicate that the customer has sent a chat response, create a file with the name ‘ClientInterface_en.properties’ in AVAYA_IC73_HOME\Webagent folder on each agent machine and add the below properties:

   task.livehelp.arrived=sounds/livehelp.wav

   livehelp.customer.action=<Path of the sound file relative to AVAYA_IC73_HOME\Webagent folder>/<Name of sound file>.wav. The sound file should be in .wav format.

2) For customizing the sound alert for an incoming chat add the below:
   task.livehelp.arrived=<Path of the sound file relative to AVAYA_IC73_HOME\Webagent folder>/<Name of sound file>.wav

Multiple Supervisor support for AARC

Till 7.3.4, only one supervisor can be assigned to a workgroup for agent contact monitoring.

With 7.3.5, the Multiple Supervisor support has been added in AIC. With this feature, multiple supervisors can be assigned to a workgroup. These assigned supervisors can monitor the agents belonging to the workgroup they are assigned to simultaneously.

As this feature has been implemented for AARC only, the other agent clients will keep supporting single supervisor monitoring.

Assigning multiple supervisors and Default Supervisor in ICManager

1. Log in to ICManager with Administrative privileges.
2. Navigate to Tools -> Groups.
3. Select the workgroup from left tree panel, right click and select the **Edit Workgroup** option.
4. Go to **Supervisor** tab.
5. Select the supervisor from **Assign from the list** on right and assign to the workgroup. The assigned supervisors will be displayed in the **Assigned Supervisors** list on the left.
6. Select the Default Supervisor from the drop-down list. By default, the first entry from the **Assigned Supervisors** will be set as the Default Supervisor.
7. Click **Ok** to save the changes.

The supervisors from the **Assigned Supervisors** list will be able to monitor an agent of this workgroup simultaneously on AARC**.**

AAWC and SDK clients will support single supervisor monitoring by using the “Default Supervisor” value.

Visual Notification for other assigned supervisors
When a supervisor starts monitoring an agent’s chat contact, the other supervisors assigned to the same workgroup gets a visual notification indicating that the agent is getting monitored. A tool-tip with the name of monitoring supervisor is also displayed.

Supervisors on WACD Admin page
Prior to 7.3.5, when an agent logged in, then the agent and as well as the agent’s supervisor was listed on WACD Admin page. The agent would be seen under “All Agents” and the supervisor will be listed in “All Supervisors”. This would happen even when no supervisor is logged in WACD.

In 7.3.5, because of list of supervisors, fetching and creating supervisor objects have been deprecated. Now, the supervisors will not be listed under “All Supervisors” unless they login into WACD explicitly.

However, only the primary supervisor will be listed in the “All Supervisors” page, even when not logged in. This is will be like existing (pre 7.3.5) behavior for primary supervisor.

OpenSSL Upgrade

OpenSSL has been upgraded from 0.9.8zc to 1.0.x. With this upgrade default protocol for SSL will be TLS 1.2 and SSLv3 protocol is no longer supported.

Refer to section “**Behavior change for SSL communication”** for more details.

ChatBlind Transfer

Blind Transfer of Chat has been added. Blind transfer is only allowed to Queue and VirtualQueues. Blind Transfer of chat to an Agent is NOT allowed.

Refer to section **“Configuration related to Chat Blind Transfer (Introduced in IC 7.3.5 FP)Chat Blind Transfer**” for more details.

Log Archiver

Following support has been added for log Archiver:

- Added filter "*-*.log" (without quotes) as a default filter/mask
- Archiving files with timestamp in their naming conventions
- Deletion of these files once retention count matches.

Failed Login Notification

In IC 7.3.5 feature pack failed login attempts are monitored and an alarm is raised based on the following configurations:

1. **TimeWindowForMaxFailedLoginAttempts:** Time in seconds with in which if M (MaxFailedLoginAttemptsInTime) successive failed login attempts are made an alarm is raised. Default: 60 seconds.
2. **MaxFailedLoginAttemptsInTime:** Number of successive login failures with in the specified time in seconds (TimeWindowForMaxFailedLoginAttempts)
   Default : 3

To set the above parameters:

a. Log in to IC Manager with Admin privileges.

b. Edit the **DirectoryServer**.

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

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

e. Enter the following values:

Name	**Value**
TimeWindowForMaxFailedLoginAttempts	60
MaxFailedLoginAttemptsInTime	**3**

f. Click **OK**.

g. Click **Apply and Ok** in **DirectoryServer** Editor.

h. Restart the **DirectoryServer** in IC Manager.

Note: It is **mandatory** to reconfigure repository database after installing IC 7.3.5 FP.

If IC repository data is not reconfigured, then system will raise alarms after 10 login attempts and after the 25th login attempt, all logins will be disabled.

If logins have been disabled, perform the steps below:

1. Restart/Update the Directory Server.
2. Reconfigure repository database .
3. Restart the Directory server.

Estimated Wait Time (EWT) for non-BA Chat

This feature presents the EWT to customer when a non-BA chat is routed to queue [Workgroup(s)], and there are no available agents. The EWT will be displayed to customer before the task is routed to agent.

Particulars:

1. EWT will be calculated (and displayed) at every route step.
   The route steps are in the WACD.Route, which is sent from chat qualification workflow to WACD.
2. EWT will be in locale of the customer's escalation.
3. EWT will not be displayed after assignment to agent.
4. EWT will not be displayed if agent will be available, and the task is routed to agent, i.e. there is no wait for customer.
5. EWT is OFF by default. Use "ewtFlavor" configuration to enable it.

EWT is calculated based on:
a. Position of the task in the workgroup's task heap (or the agent's task heap).
A task "heap" is a sorted list of tasks.
b. Number of tasks routed to all the agents of that workgroup.
c. Average of (a) and (b), if routed to multiple workgroups/agents.
d. The above (c), is used to arrive at EWT using the Average Agent handling Time (AAHT).

The AAHT is maintained using the handling time of all chat tasks.

Enhancements in IC 7.3.4 Service Pack

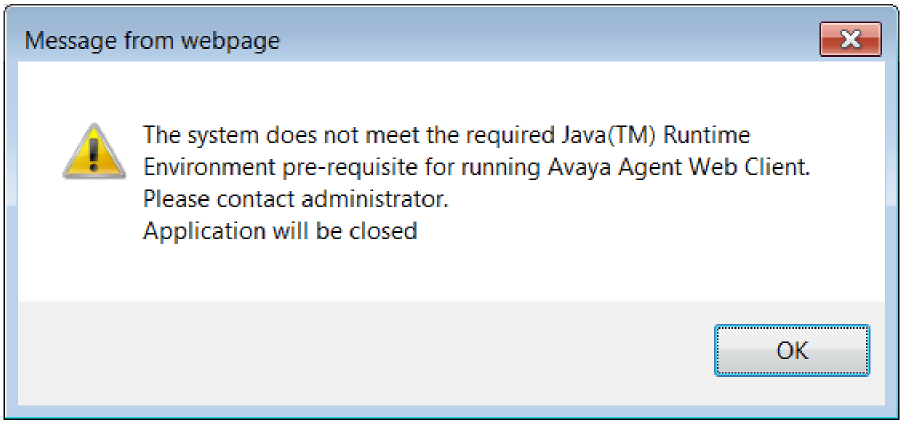
Java Upgrade

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 the 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.


Message from webpage

The system does not meet the required Java(TM) Runtime Environment pre-requisite for running Avaya Agent Web Client.
Please contact administrator.
Application will be closed

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. Log in to IC Manager with Admin privileges.

b. Edit the DS.

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

d. Click **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.
This property is obsolete from IC release 7.3.5.

Idle Timeout Tenant Properties Support

Note: Make sure that configuration from "Configuration for Inactivity timeout for Chat Disconnect (Introduced in IC 7.3.2 FP)" section is done.

`<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

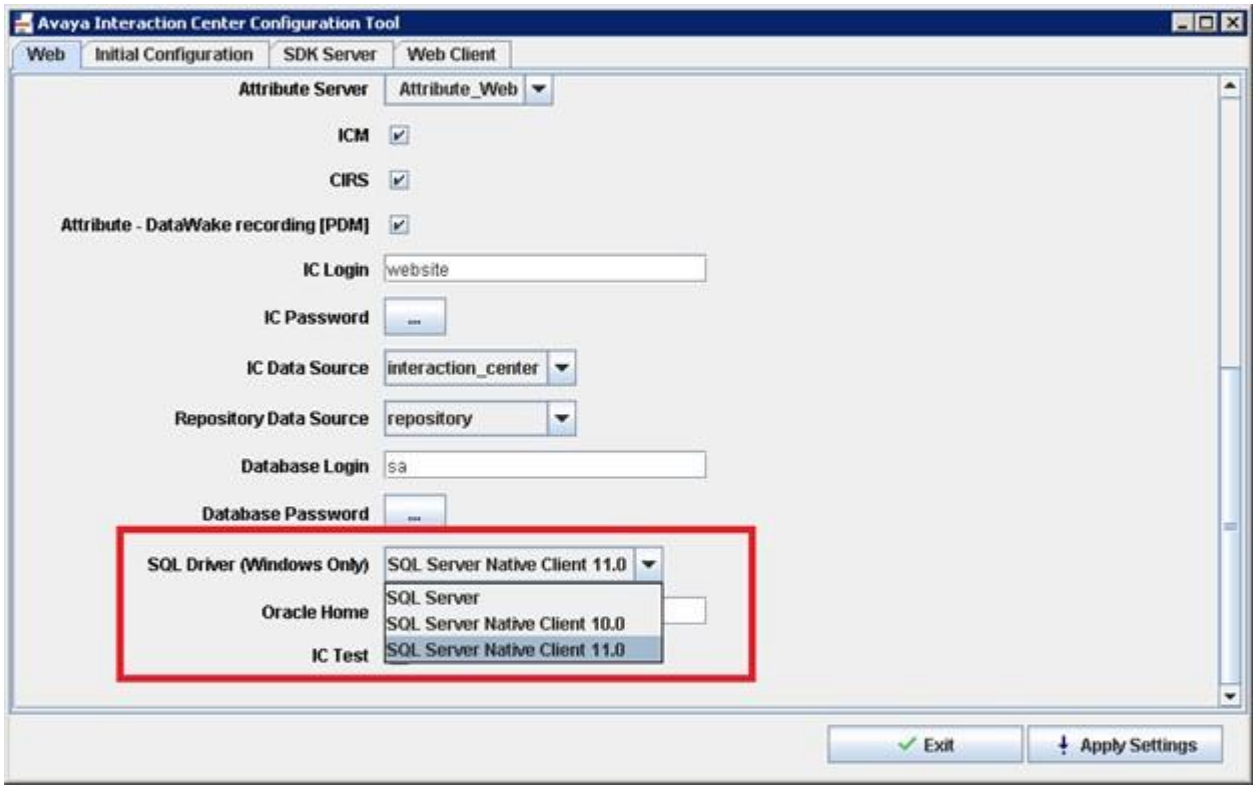
When you configure the website in IC, the Config tool creates DSN for PDM to communicate with the database.
Earlier, you could create these DSNs with the default ODBC driver, SQL Server, which is shipped with the Windows operating system. Now, Microsoft has deprecated the driver and cannot support it in future versions of Microsoft Windows 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.



Attribute Server: Attribute_Web

ICM ☑

CIRS ☑

Attribute - DataWake recording [PDM] ☑

IC Login: website

IC Password: ...

IC Data Source: interaction_center

Repository Data Source: repository

Database Login: sa

Database Password: ...

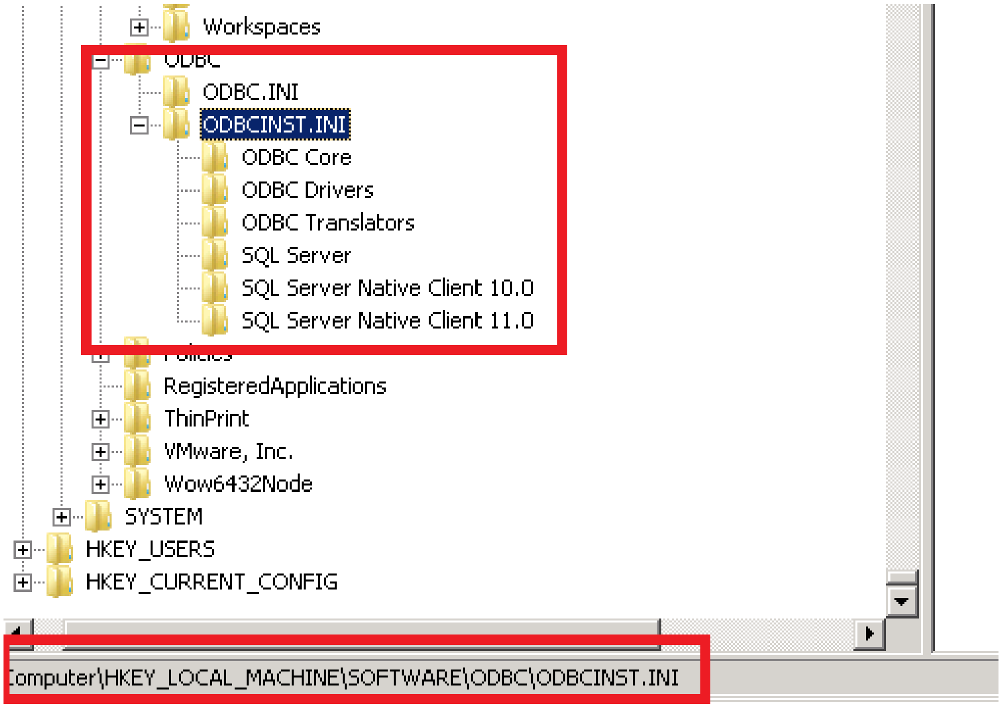
SQL Driver (Windows Only): SQL Server Native Client 11.0

- SQL Server
- SQL Server Native Client 10.0
- SQL Server Native Client 11.0

Oracle Home

IC Test

Note: You can also access the registry to verify the installed ODBC drivers.



```
Workspaces
ODBC
    ODBC.INI
    ODBCINST.INI
        ODBC Core
        ODBC Drivers
        ODBC Translators
        SQL Server
        SQL Server Native Client 10.0
        SQL Server Native Client 11.0
Policies
RegisteredApplications
ThinPrint
VMware, Inc.
Wow6432Node
SYSTEM
HKEY_USERS
HKEY_CURRENT_CONFIG
```

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBCINST.INI

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).

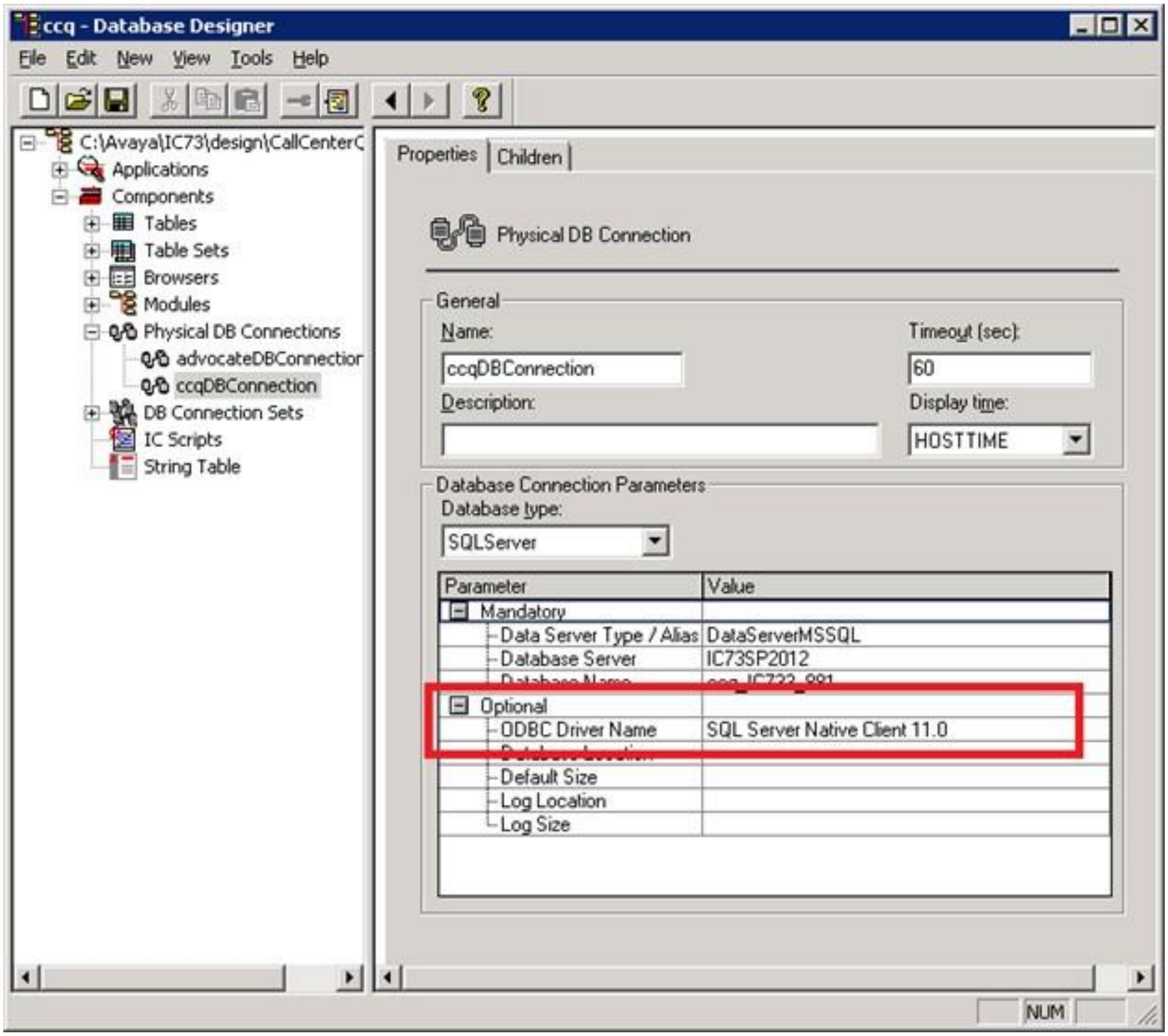
Note: This option will be removed in future builds.

- 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.



General

Name: ccqDBConnection

Timeout (sec): 60

Description:

Display time: HOSTTIME

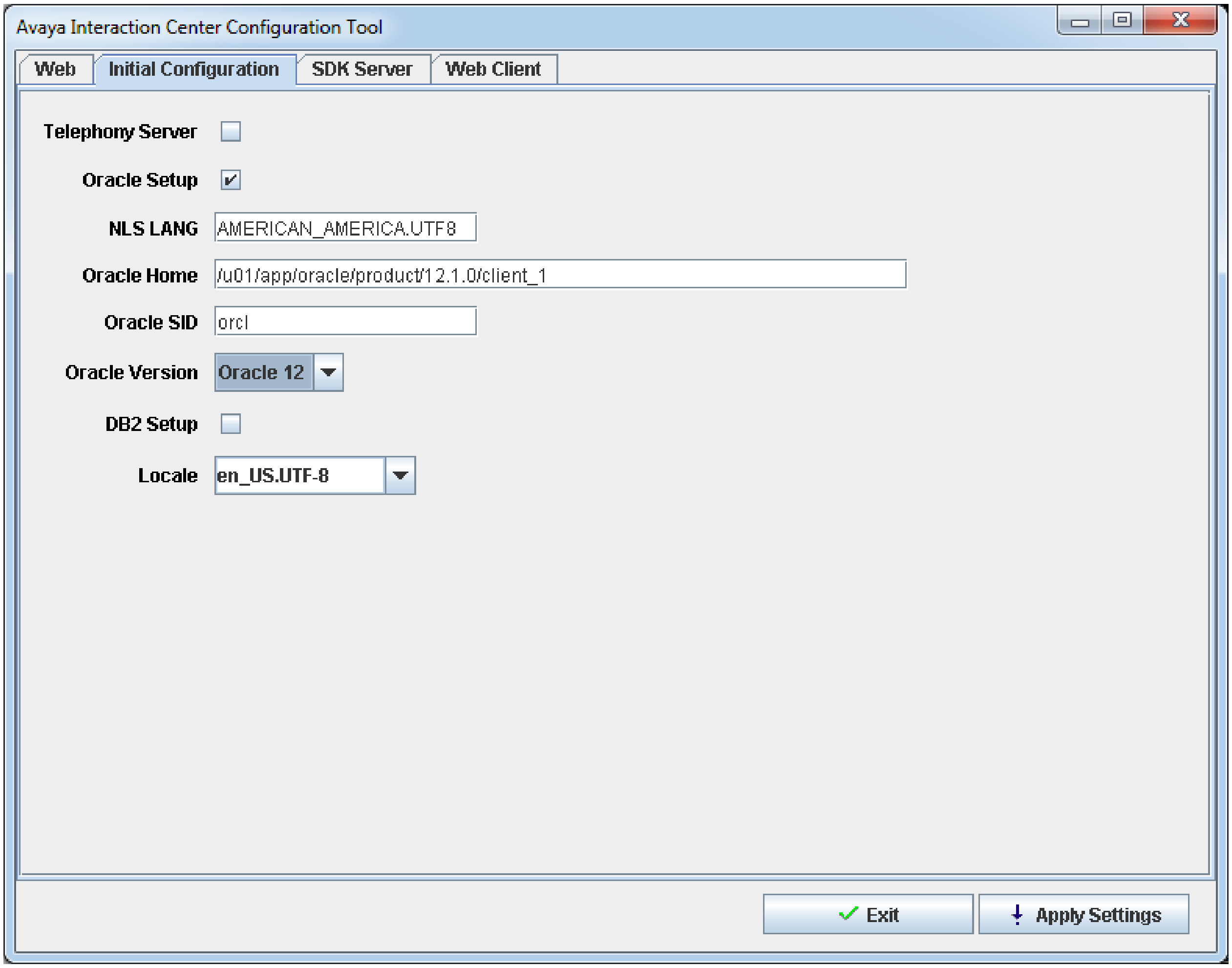
Database Connection Parameters

Database type: SQLServer

Parameter	Value
Mandatory	
Data Server Type / Alias	DataServerMSSQL
Database Server	IC73SP2012
Database Name	ccq_IC733_001
Optional	
ODBC Driver Name	SQL Server Native Client 11.0
Database Location	
Default Size	
Log Location	
Log Size	

Oracle 12C database

In the Avaya IC Configuration Tool a new Oracle version is added. The **Oracle Version** field displays Oracle 12.



Telephony Server ☐

Oracle Setup ☑

NLS LANG AMERICAN_AMERICA.UTF8

Oracle Home /u01/app/oracle/product/12.1.0/client_1

Oracle SID orcl

Oracle Version Oracle 12

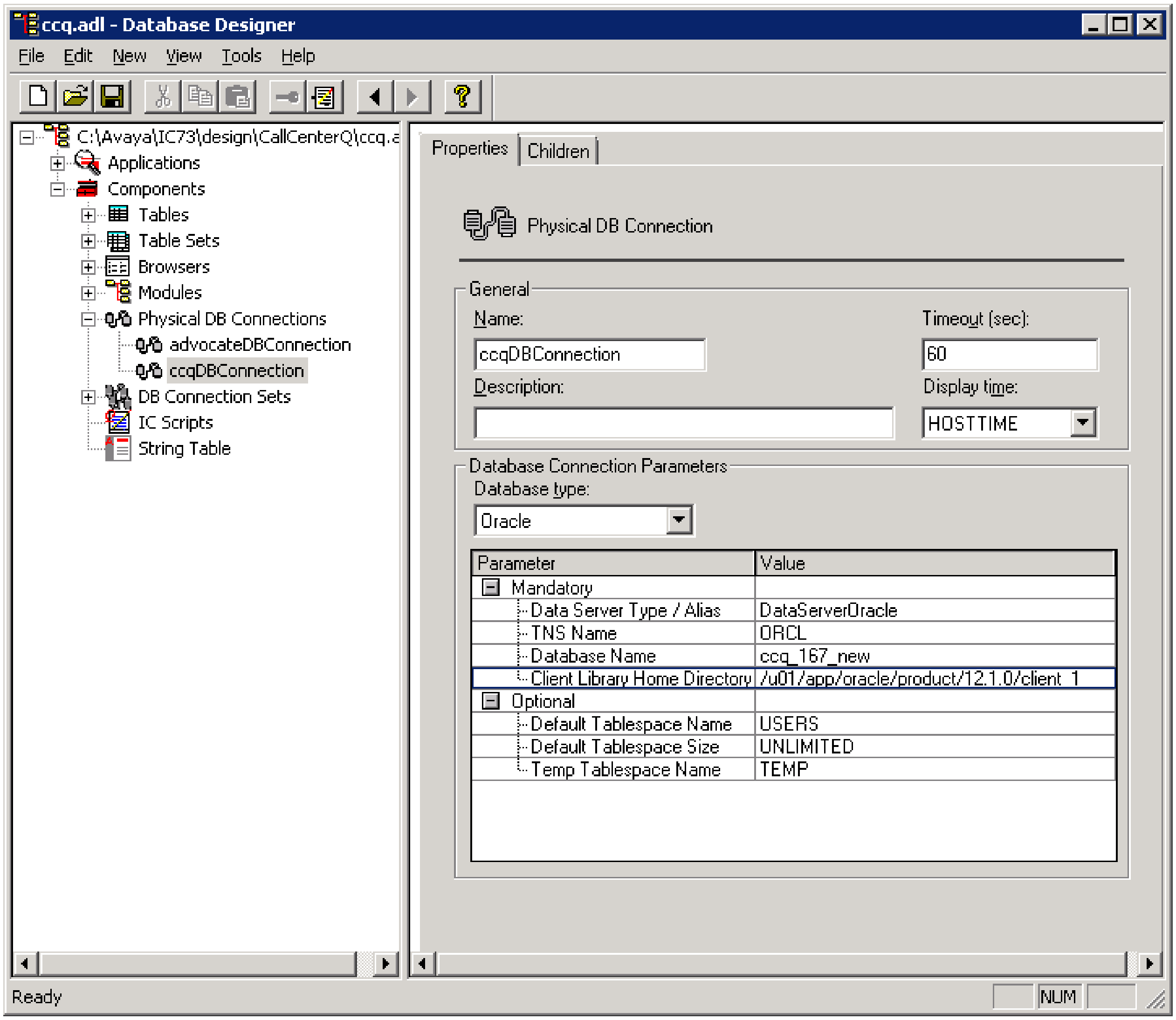
DB2 Setup ☐

Locale en_US.UTF-8

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.



General

Name: ccqDBConnection

Timeout (sec): 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

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 Windows 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:

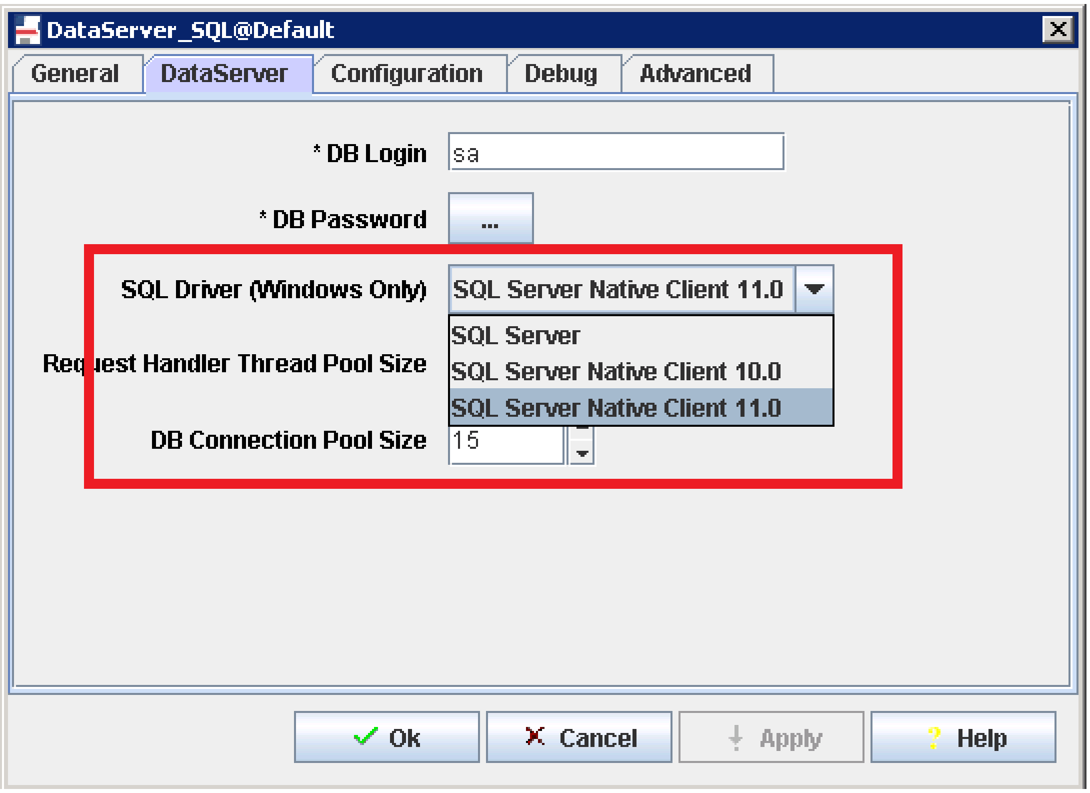
- SQL Server (Installed with Windows OS).

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.



* DB Login: sa

* DB Password: ...

SQL Driver (Windows Only): SQL Server Native Client 11.0

Request Handler Thread Pool Size

DB Connection Pool Size: 15

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 Windows 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.

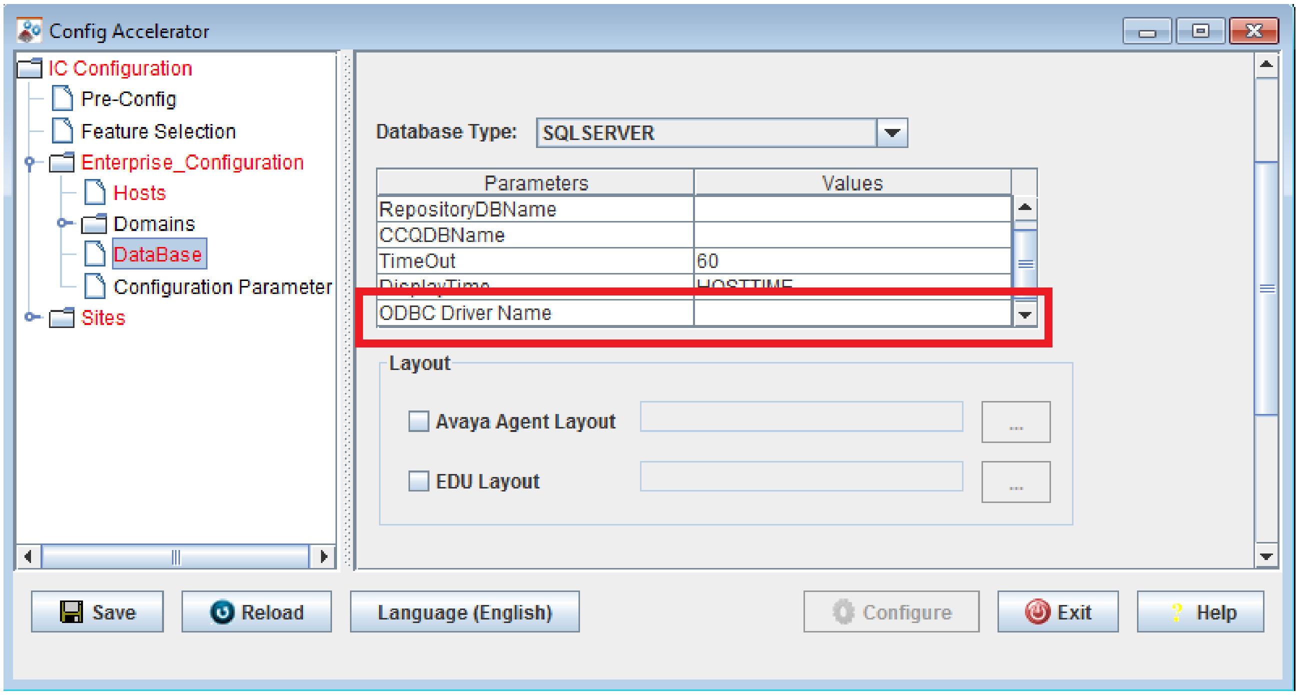
In Config Accelerator, you can view the new parameter ODBC Driver Name on the Properties tab. For this parameter, you must manually enter the appropriate value from the following options:

- 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).



Database Type: SQLSERVER

Parameters	Values
RepositoryDBName	
CCQDBName	
TimeOut	60
DisplayTime	HOSTTIME
ODBC Driver Name	

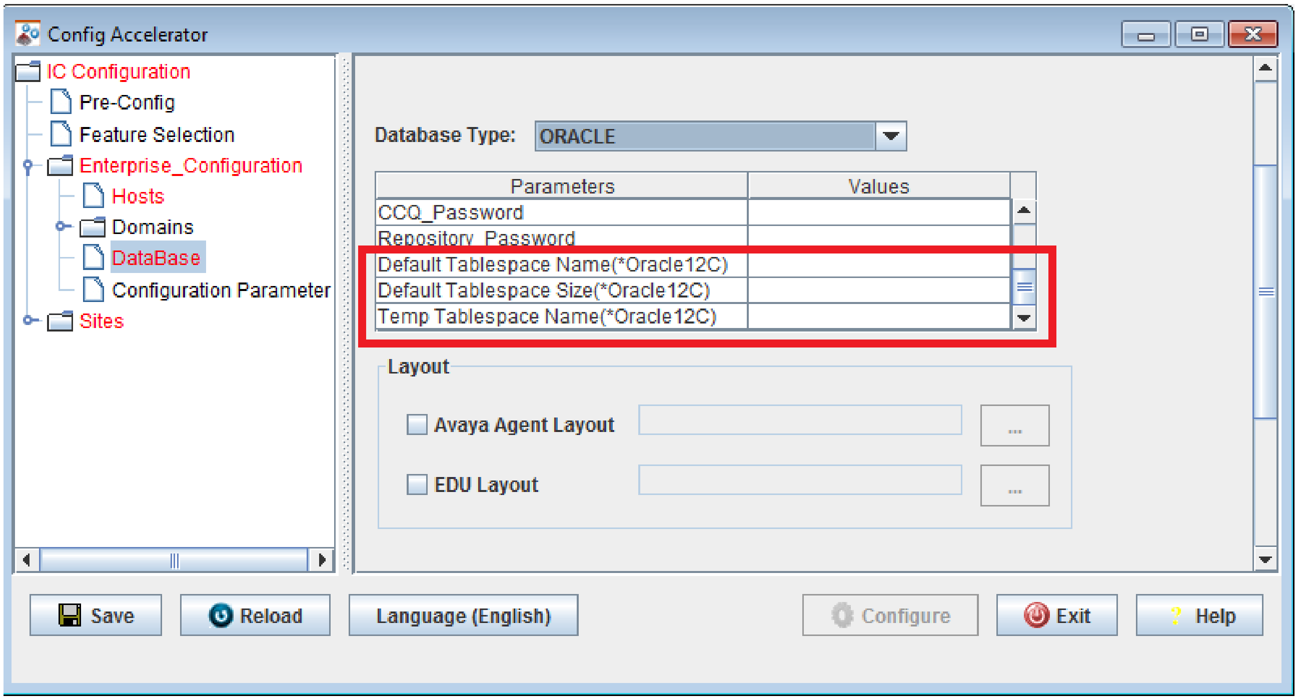
☐ Avaya Agent Layout

☐ EDU Layout

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)



Database Type: ORACLE

Parameters	Values
CCQ_Password	
Repository_Password	
Default Tablespace Name(*Oracle12C)	
Default Tablespace Size(*Oracle12C)	
Temp Tablespace Name(*Oracle12C)	

Configuring IC with new database

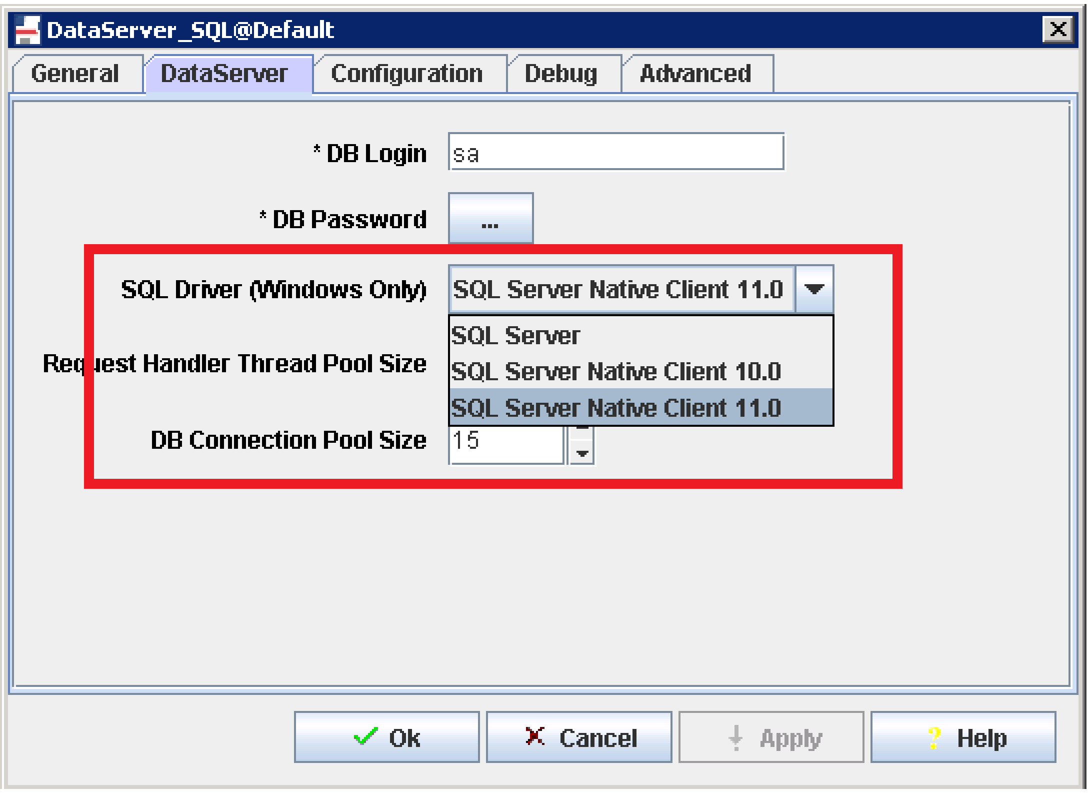
Fresh Installation

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.



* DB Login: sa

* DB Password: ...

SQL Driver (Windows Only): SQL Server Native Client 11.0

- SQL Server
- SQL Server Native Client 10.0
- SQL Server Native Client 11.0

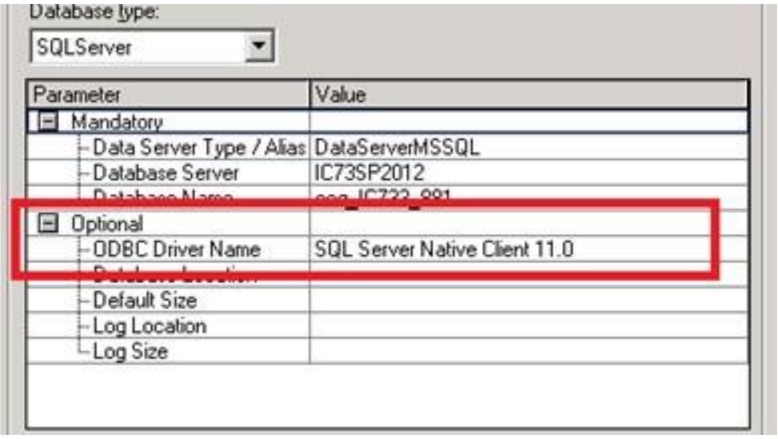
Request Handler Thread Pool Size

DB Connection Pool Size: 15

5. Run DB Designer.

6. Add required details for SQL server.

7. Add entry for ODBC driver name.



Database type: SQLServer

Parameter	Value
Mandatory	
Data Server Type / Alias	DataServerMSSQL
Database Server	IC73SP2012
Database Name	ccq_IC733_881
Optional	
ODBC Driver Name	SQL Server Native Client 11.0
Database Location	
Default Size	
Log Location	
Log Size	

8. Configure database for both ccq and repository.

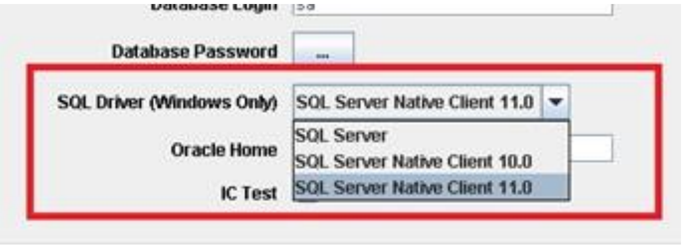
To verify which ODBC driver name is used by DataServer, verify in the logs for dbHome:

```
!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.



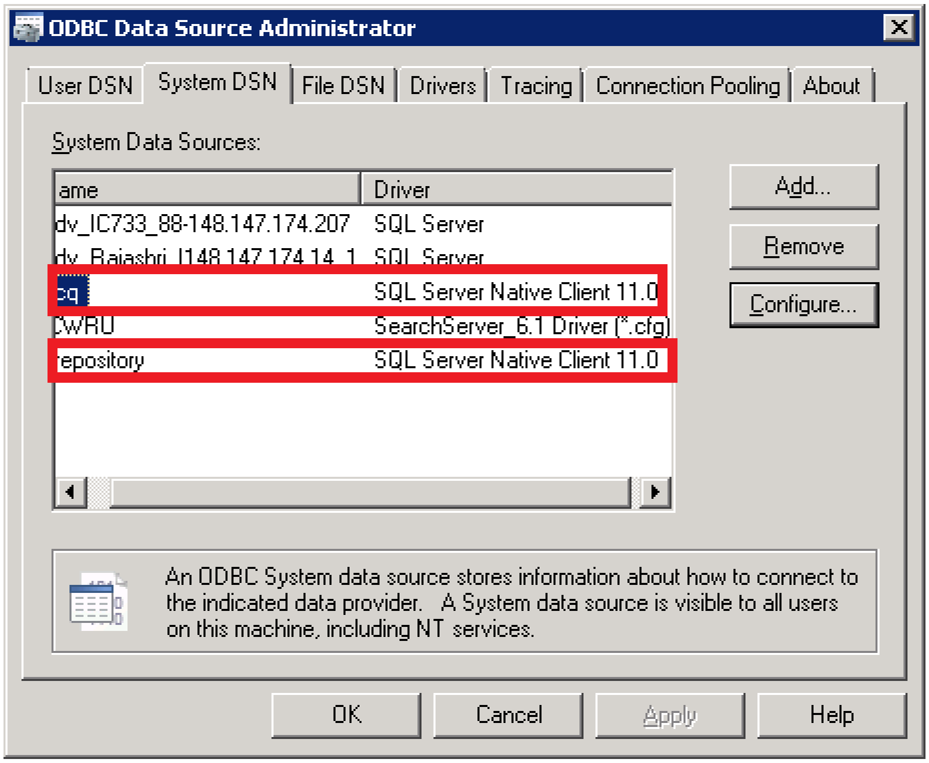
Database Password: ...

SQL Driver (Windows Only): SQL Server Native Client 11.0

- SQL Server
- SQL Server Native Client 10.0
- SQL Server Native Client 11.0

11. Apply settings in Avaya IC Configuration Tool.

12. Verify that DSNs are created with the correct ODBC drivers.



ODBC Data Source Administrator

System Data Sources:

ame	Driver
dv_IC733_88-148.147.174.207	SQL Server
dv_Rajashri_I148.147.174.14_1	SQL Server
cq	SQL Server Native Client 11.0
CWRU	SearchServer_6.1 Driver (*.cfg)
epository	SQL Server Native Client 11.0

An ODBC System data source stores information about how to connect to the indicated data provider. A System data source is visible to all users on this machine, including NT services.

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.
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.

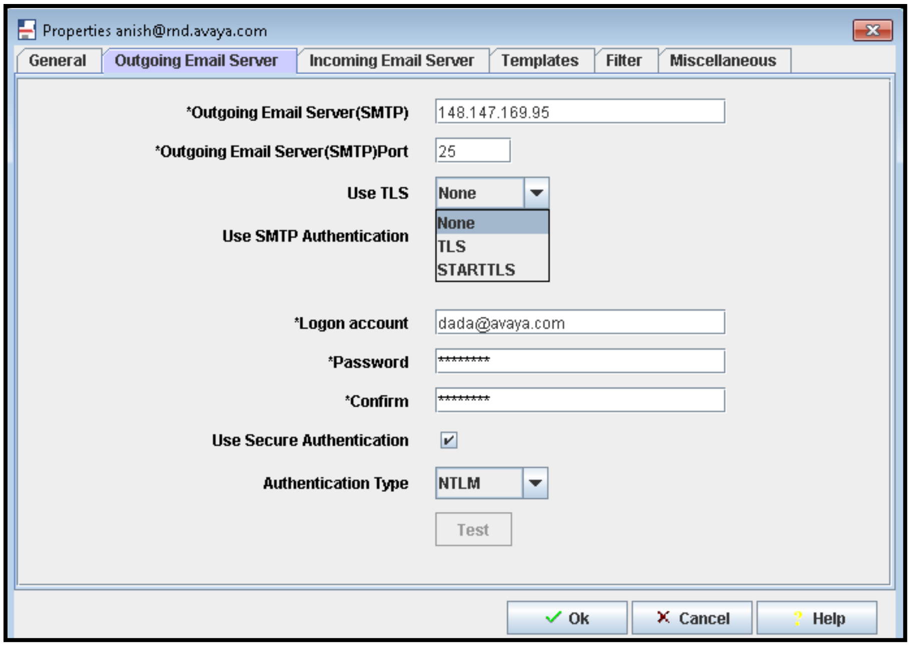
Currently IC Manager has the provision to provide Outgoing Email Server (SMTP) information with the default port used as “25”.

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:
      - NTLM
      - CRAMMD5
      - LOGIN

New fields added for supporting the SMTP & SSL support:



*Outgoing Email Server(SMTP) 148.147.169.95

*Outgoing Email Server(SMTP)Port 25

Use TLS None

- None
- TLS
- STARTTLS

Use SMTP Authentication

*Logon account dada@avaya.com

*Password *********

*Confirm *********

Use Secure Authentication ☑

Authentication Type NTLM

Test

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

Column Name	The Outgoing Email Server tab in IC Manager
smtppassword	Password
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

As a part of this enhancement the chat messages shown at the agent end would contain time stamp.

Design:

The chat messages are broadcast by the ICMserver. So when a chat message is sent by the agent or customer, ICM Server adds a UTC time as a new parameter with the Transcript object. Depending on the time zone of the client machine, the client 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, or 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.

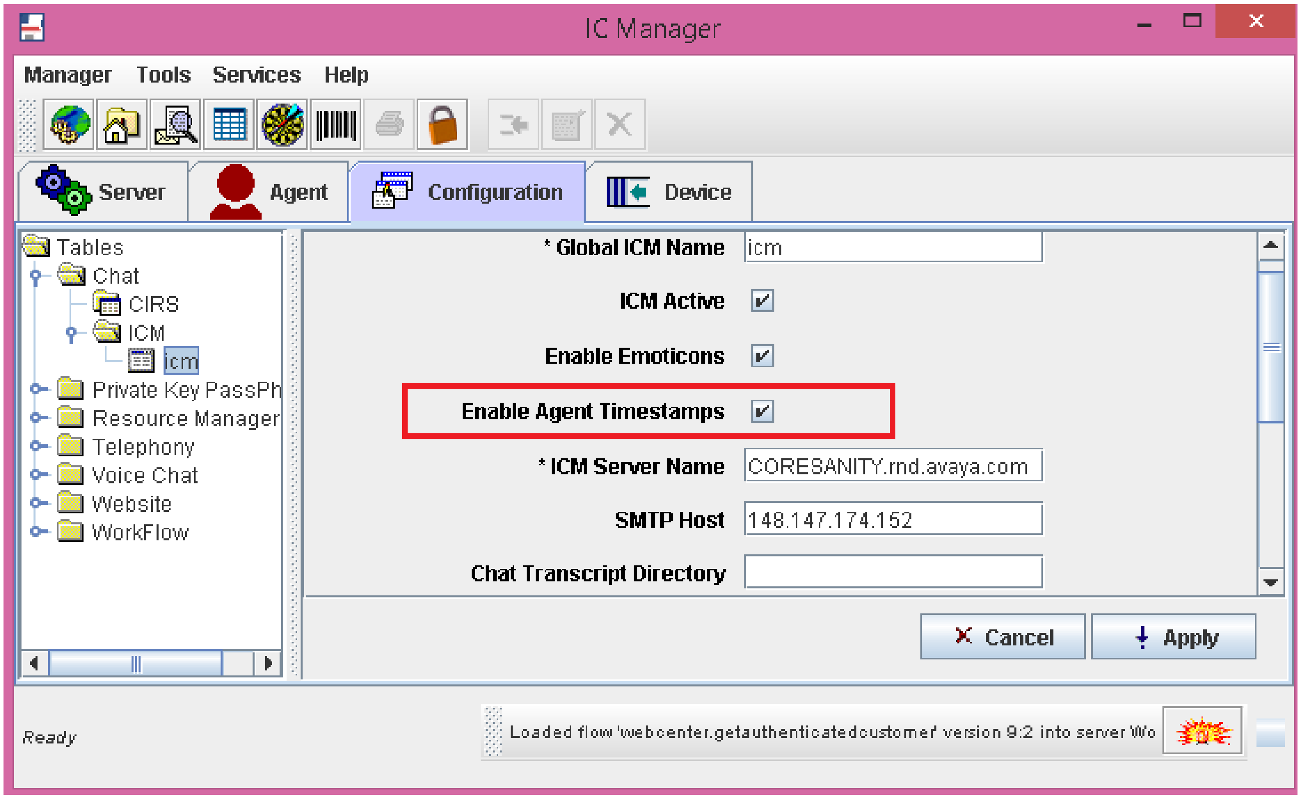
3. Go to the **IC Manager Configuration** tab.

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.



* Global ICM Name: icm

ICM Active ☑

Enable Emoticons ☑

Enable Agent Timestamps ☑

* ICM Server Name: CORESANITY.rnd.avaya.com

SMTP Host: 148.147.174.152

Chat Transcript Directory:

Ready

Loaded flow 'webcenter.getauthenticatedcustomer' version 9:2 into server Wo

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:

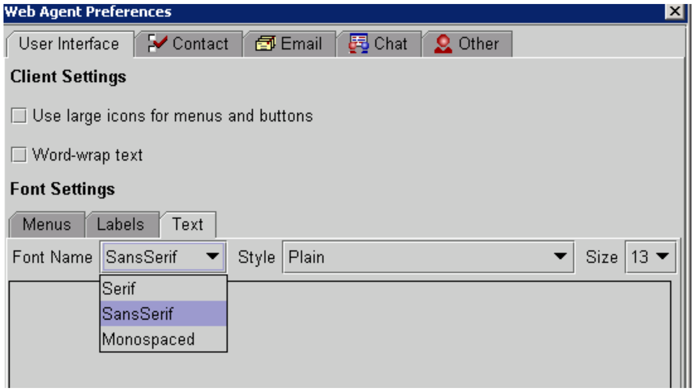
- Avaya ASGPlugin requires Administrative privileges to install.
- A reboot of the operating system after installation of ASGPlugin is required to complete the installation.
- From computer properties, clear **Allow connections only from computers running Remote Desktop with Network Level Authentication** 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



Client Settings

□ Use large icons for menus and buttons

□ Word-wrap text

Font Settings

Font Name SansSerif Style Plain Size 13

You can change the fonts in **Tools** > **Preferences** > **User Interface** > **Text**. To see the change in font, 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, a 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 the Configuration section for configuration of the threshold values.

Enhancements in IC 7.3.2 Feature Pack

New Features and Enhancements

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

Security Enhancements

There are a number of security enhancements introduced in IC 7.3.2 FP. The main enhancements are:

- Introduced a mechanism to prevent Cross-Site Scripting, man-in-middle attacks
- Introduced the logout option in IC Admin website
- Introduced a mechanism to prevent 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:

- Interpreting 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, it becomes difficult 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:

- 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 bit, 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 Microsoft Windows platform

Perform the following steps on the computer where the IC WebServices service is configured for Microsoft 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.

The 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

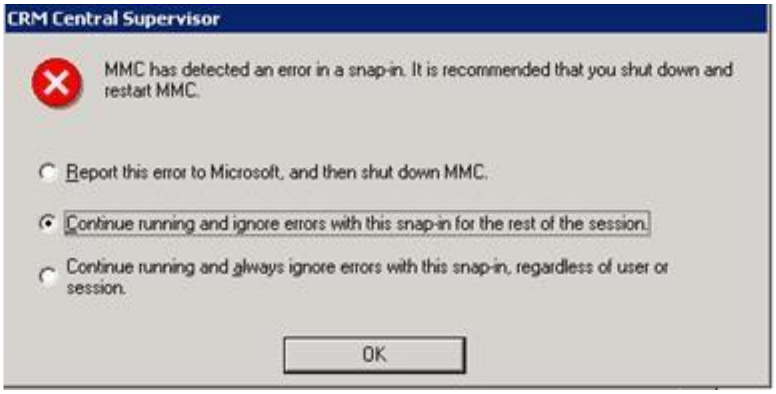
Crash dump on Windows platform

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 j`ava[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.

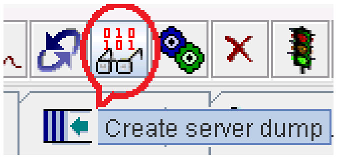
Using the Simplified IC Dump feature, IC administrators can create core dump of any running IC server configured in IC Manager. You can create, through the IC Manager, the core dump of a running IC server by selecting single or multiple servers and clicking **Create server dump** on the Toolbar.
The 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, 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 ofthe 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 forthat 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:

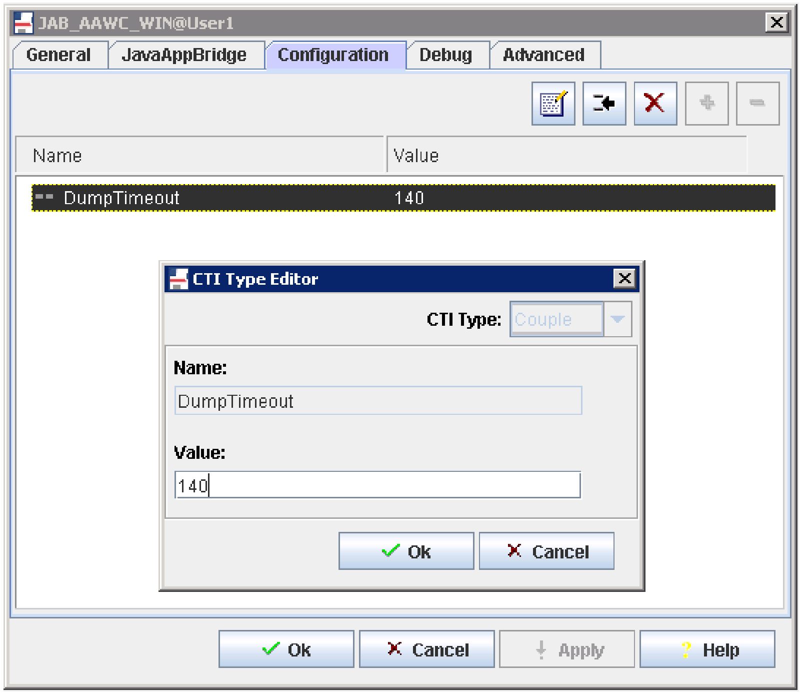
1. By launching a separate utility as a separate process and providing a process ID of the selected server as an argument to that utility process, you can create dump of a runningserver. The Simplified IC Dump feature uses `<AVAYA_IC73_HOME>\bin\avayadmp.exe`, gcore and gencore utilities for core dump 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.



Name	Value
DumpTimeout	140

CTI Type: Couple

Name: DumpTimeout

Value: 140

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 Microsoft 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.

Command	Description
	If not provided, then the system creates a full dump.
-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`
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.

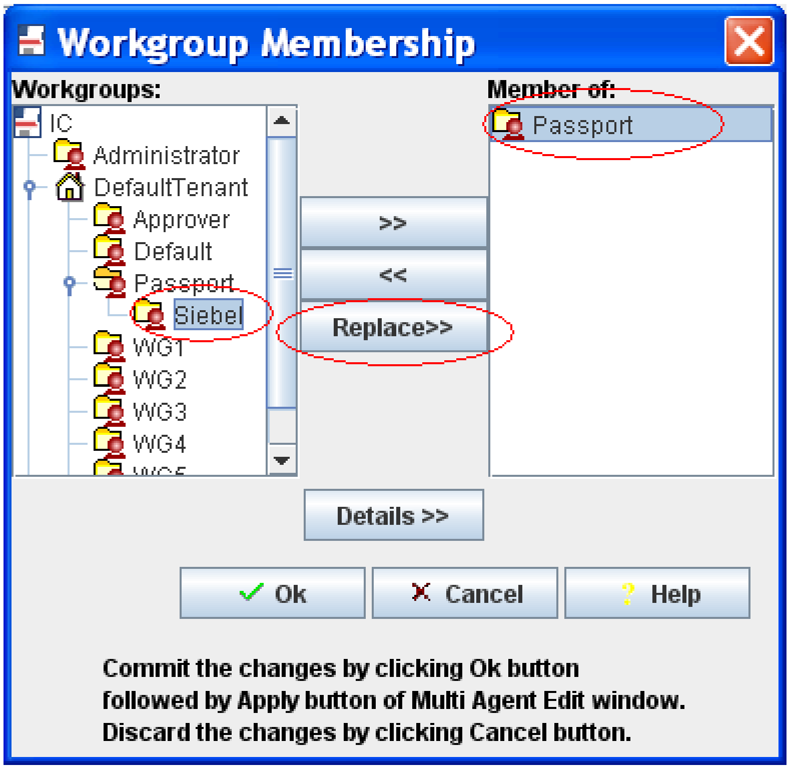
In the **Workgroup Membership** window, a new button **Replace>>** was added.

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>>**.



Commit the changes by clicking Ok button
followed by Apply button of Multi Agent Edit window.
Discard the changes by clicking Cancel button.

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

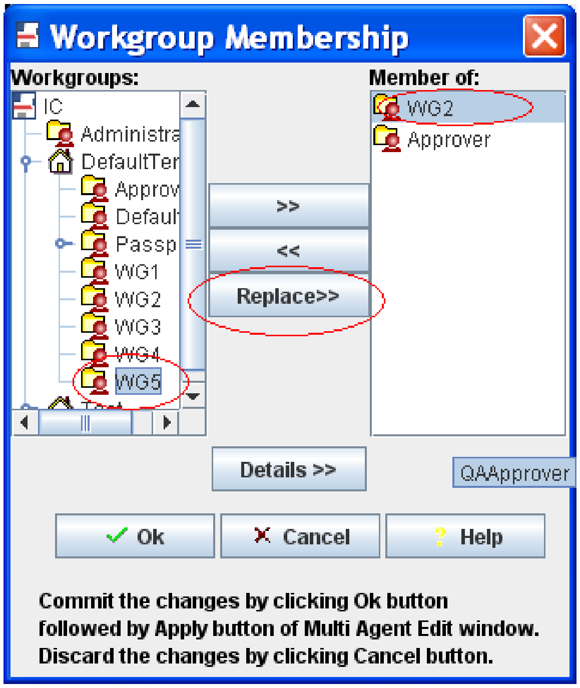
Scenario 2:

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:

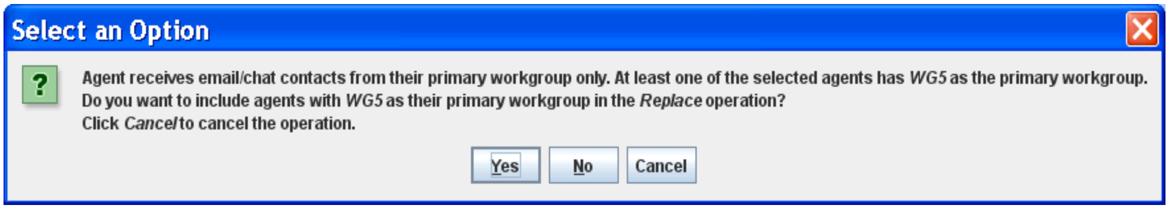
1. Select the original workgroup from the **Member of** list on the right side of the window.
2. Select the new workgroup from **Workgroups** list on the left side of the window.
3. Verify that all three buttons **>>** (Add), **<<** (Remove) and **Replace>>** are active.

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



Commit the changes by clicking Ok button followed by Apply button of Multi Agent Edit window. Discard the changes by clicking Cancel button.

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:



Agent receives email/chat contacts from their primary workgroup only. At least one of the selected agents has *WG5* as the primary workgroup.
Do you want to include agents with *WG5* as their primary workgroup in the *Replace* operation?
Click *Cancel* to cancel the operation.

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

Agent	Workgroup	Value of the workgrouporder field in the groupmember table
agent3	WG5	0
	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 7.3.10 Installation

This section describes the SP Installer that updates the existing Avaya IC 7.3 systems with the Avaya IC 7.3.10 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 7.3.10 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/7.3.10/<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.

Chapter 3: Installation

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 pop up 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 7.3.10 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 the Microsoft 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 7.3.10 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 7.3.8 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

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

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

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

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

4. 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.

5. Press **Enter**.

Possible issues related to Windows Server 2019

Problem

On Windows Server 2019 the Service Pack installer doesn't run

Solution

Disable all exploit protection options that can affect Java.

- Go to the Windows Defender Security Center, Apps & browsers control, Exploit protection, program setting, disable the appropriate options for java.exe. On a default Windows setup, the options you need to override are:
  1. Control flow guard
  2. Data Execution Prevention
  3. Randomize memory allocations
  4. Validate exception chains
  5. Validate heap integrity
- Apply all changes.

After installing the SP, all the overrides may be discarded.

Problem

Business Advocate Administration console (BAA): Windows ActiveX errors appear

Solution

1) Switch off exploit protection
- Go to the Windows Defender Security Center, Apps & browsers control, Exploit protection, System setting

Item	Change to
Control flow guard (CFG)	Off by default
Data Execution Prevention (DEP)	Off by default
Force randomization for images (Mandatory ASLR)	Off by default
Randomize memory allocations (Bottom-up ASLR)	Off by default
High-entropy ASLR	Use default (On)
Validate exception chains (SEHOP)	Off by default
Validate heap integrity	Off by default

- If you have AIC installed and configured, just stop IC and restart the machine. Ignore the step 2.

2) Install Avaya Interaction Center
3) Configure Business Advocate
4) After BA configuration to check registry branch
   HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\MMC\SnapIns\{20D604E0-6E00-11D2-A94C-00A0C985986D}
   This branch must exist. This is necessary for correct work of Advocate Component Manager.

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`.

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, take 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
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 7.3.10

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 7.3.10

The following are the prerequisites for AAWC:

- The machine on which the AAWC is launched in the browser should have 32-bit Oracle JRE 1.8.0.121 or higher 1.8 version.
- Only one instance of JRE should be installed and enabled.

Prerequisites for CVLAN Client in IC 7.3.10

The Telephony Server in IC 7.3.9 has been upgraded to use AES cvlan library 8.1.3. If you do an upgrade to IC 7.3.10 from Release 7.3.8 or earlier, all the TS servers should be upgraded to AES CVLAN client 8.1.3 or above.

Prerequisites for installing IC 7.3.10

This section describes the prerequisites for installing the IC 7.3.10 Service Pack.

1. Before you install IC 7.3.10, you must have IC 7.3 installed on your system. IC 7.3.10 upgrade is also supported from IC 7.3.1 SP or IC 7.3.2 FP or IC 7.3.3 FP or IC 7.3.4 SP or IC 7.3.5 FP or IC 7.3.6 SP or IC 7.3.7 SP or IC 7.3.8 SP or IC 7.3.9 SP.

Getting Started

Avaya IC 7.3.10 is available on the Avaya Support website at: http://support.avaya.com/downloads/

To receive the IC 7.3.10 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 based on MAC address of the server and then upgrade the IC and OA from the version 7.3.8 or an earlier release, your license key will not be valid.

WebLM 7.0.1 has changed the way License is generated based on MAC IDs for VMware (Virtualizations) based WebLM Servers. The Licenses has to be generated based on the hostID that we will get from the WebLM URL.You have to request a replacement license.This request is described in “AIC Installation Planning and Prerequisites guide” document, chapter 8:”Interaction Center Licensing”, section “Requesting a replacement license file”, https://downloads.avaya.com/css/P8/documents/100159305

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 7.3.10 Service Pack

You can download the IC 7.3.10 Service Pack files from the Avaya Support site: http://support.avaya.com/downloads/.

To download IC 7.3.10, 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 7.3.10 file name to download the respective file.
7. Move the IC 7.3.10 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 7.3.10 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	`IC7310WinAdmin.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	`IC7310WinAgentClient.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	`IC7310WinWebClient.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 Connector	Windows Solaris	`IC7310WinWebConnector.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. `IC738SolWebConnector.tar`. Extract the files into the install folder on the local computer.
IC Servers	Windows Solaris AIX	`IC7310WinServer.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. `IC738SolServer.tar`. Extract the files into the install folder on the local computer. `IC732AixServer.tar`. Extract the files into the install folder on the local computer.

Component/computer	Operating System	File name
Siebel Integration component (IC side)	Windows Solaris AIX Linux	ICSide7310win.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. ICSide738SolServer.tar. Extract the files into the install folder on the local computer. IC732AixServer_Openssl1.xUpgrade_patch.tar. Extract the files into the install folder on the local computer. ICSide738Linux.tar. Extract the files into the install folder on the local computer.
Siebel Integration component (Siebel side)	Windows Solaris AIX Linux	SiebelSide7310win.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. SiebelSide738SolServer.tar. Extract the files into the install folder on the local computer. SiebelSide732aix.tar. Extract the files into the install folder on the local computer. SiebelSide738Linux.tar. Extract the files into the install folder on the local computer.
IIS	Windows	IC7310WinIIS.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.

Installation options

Avaya IC 7.3.10 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 7.3.10 from a shared network computer to upgrade other computers without having to copy the IC 7.3.10 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 SP 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 Service 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`
Solaris	`./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

Log Archiver Service (For windows platform only):

The Log Archiver is installed by the pre-install script of the following IC 7.3.10 components:

- Windows Server installation
- Administration and Design installation
- Avaya Agent (rich client) installation

The log archiver is by default installed in either ‘C:\Program Files’ or ‘C:\Program Files (x86)’depending on whether the OS is 32 bit or 64 bit, respectively. In case, you wish to install the log archiver at a different location, it should be installed before installing the respective IC component. This is not a mandatory step.

Follow the bellow steps to install the log archiver:

1) Ensure dot net framework 3.5 SP1 is installed on the system.
2) Run the AvayaLogSaverSetup.exe available in the installer. You will be prompted to enter the install location.
3) Complete the installation.

IC Components:

After you complete the instructions for a network installation or a local installation, install the IC 7.3.10components 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 7.3.10 Server component. Since IC 7.3.9, the Server component can be installed on the Windows platform only.

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 SP 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 `IC7310WinServer.zip` file.
3. Copy the IC7310WinServer 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 IC7310WinServer folder and double-click `setupwin32.exe` to start the installation program.
   b. At the Welcome screen, click **Next**.
   c. The next screen displays the License Agreement.
   d. Select the **I accept the terms in the license agreement** option, click **Next**.
   e. The next screen displays the location of the Uninstall program, click **Next**.
   f. In the dialog box that prompts **Please stop all Avaya IC servers and services**, click **Continue**.
   g. 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\7.3.10\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\7.3.10\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 SP 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 `IC738SolServer.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 License Agreement.

6. Select the **I accept the terms in the license agreement** option, click **Next**.

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

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

9. 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:	If installation is unsuccessful, the system displays:
Installation was successful. No errors or warnings were generated. Complete log messages are available at: .../IC73/ICServicePacks/7.3.10/Server/Log/install.log	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/7.3.10/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 SP 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. The next screen displays the License Agreement.

h. Select the **I accept the terms in the license agreement** option, click **Next**.

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

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

k. 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

l. Click **Finish**.

m. 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 7.3.10 release. The Siebel Integration component is installed on the Windows 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 `SiebelSide7310win.zip` file.

2. Open the SiebelSide7310win 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 License Agreement.

5. Select the **I accept the terms in the license agreement** option, click **Next**.

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

   For example, C:\seaxx\siebsrvr.

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

8. 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**.

9. 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\7.3.10\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: C:\Seaxxx\siebsrv\ICServicePack\7.3.10\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 `ICSide7310win.zip` file.

2. Open the ICSide7310win 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 License Agreement.

5. Select the **I accept the terms in the license agreement** option, click **Next**.

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

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

8. 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\7.3.10\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\7.3.10\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

Solaris is not supported since IC 7.3.9

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 SiebelSide738sol.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. The next screen displays the License Agreement.

6. Select the **I accept the terms in the license agreement** option, click **Next**.

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

For example, `root/seaxx/siebsrvr`.

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

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

10. 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/7.3.8/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/7.3.8/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 `ICSide738sol.tar` file.

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

3. Press **Enter**.

4. On the Welcome screen, click **Next**.
5. The next screen displays the License Agreement.
6. Select the **I accept the terms in the license agreement** option, click **Next**.
7. On the next screen, enter the path location for the IC Servers installation and click **Next**.

   For example, `root/IC73`.

8. On the next screen displays the location of the Uninstall program, click **Next**.
9. 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**.
10. 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/7.3.8/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/7.3.8/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 SiebelSide738aix.tar file.

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

c. Press **Enter**.

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

e. The next screen displays the License Agreement.

f. Select the **I accept the terms in the license agreement** option, click **Next**.

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

For example, root/seaxx/siebsrvr

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

i. 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**.

j. 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/7.3.8/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/7.3.8/SiebelSide/Log/install.log LIST OF ERRORS AND WARNINGS

k. Click **Finish**.

l. 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 ICSide732aix.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. The next screen displays the License Agreement.

f. Select the **I accept the terms in the license agreement** option, click **Next**.

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

For example, root/IC73.

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

i. 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**.

j. 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: Installation was successful. No errors or warnings were generated. Complete log messages are available at: .../IC73/ICServicePacks/7.3.2/ICSideSiebel/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/7.3.2/ICSideSiebel/Log/install.log LIST OF ERRORS AND WARNINGS

k. 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 7.3.10 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 7.3.10 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 `IC7310WinWebConnector.zip` file.

3. Open the IC7310WinWebConnector 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 License Agreement.

6. Select the **I accept the terms in the license agreement** option, click **Next**.

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

8. 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\7.3.10\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\7.3.10\WebConnector\Log\install.log LIST OF ERRORS AND WARNINGS

5. Click **Finish**.

   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 `IC738SolWebConnector.tar` file.
3. At the command prompt, type: `./setupsolarisSparc.bin`.
4. Press **Enter**.
5. At the Welcome screen, click **Next**.
6. The next screen displays the License Agreement.
7. Select the **I accept the terms in the license agreement** option, click **Next**.
8. On the next screen, which displays the location of the Uninstall program, click **Next**.
9. 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/7.3.10/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/7.3.10/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 7.3.10 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 7.3.10 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 `IC7310WinWebClient.zip` file.
2. Open the IC7310WinWebClient 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 License Agreement.
5. Select the **I accept the terms in the license agreement** option, click **Next**.
6. The next screen 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 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:	If installation is unsuccessful, the system displays:
Installation was successful. No errors or warnings were generated. Complete log messages are available at: ...\IC73\ICServicePacks\7.3.10\WebClient\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\7.3.10\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 7.3.10 Administration and Design component. Only the Windows platform supports the IC 7.3.10 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 `IC7310WinAdmin.zip` file.

3. Copy the IC7310WinAdmin 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 IC7310WinAdmin 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 License Agreement.

   e. Select the **I accept the terms in the license agreement** option, click **Next**.

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

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

   h. 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\7.3.10\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\7.3.10\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.

Note: During IC 7.3.10 installation you can see following error: “Error unregistering the component TreeCtrl.ocx”. It does not affect the installation, you can ignore it. To prevent this error, do the following cmd command before IC 7.3.10 insallation:

[IC_HOME]\bin> regsvr32 treectrl.ocx

Avaya Agent (rich client) installation

This section describes the installation procedures for the IC 7.3.10 Avaya Agent (rich client) component. Only the Windows operating system supports the Avaya Agent installation.

Note: You can install the IC 7.3.10 Avaya Agent (rich client) component after you have installed and configured all other IC 7.3.10 SP components. You do not require stopping the IC Servers before installing the IC 7.3.10 Avaya Agent (rich client) component.

Note: Before upgrading from 7.3.x Release Version to 7.3.10, make sure that all OCX files have been registered. To check this, to run the file [RichClient_Home]\bin\RegRichClient.bat with administrator rights. Afterwards you can start 7.3.9 installation. If some files haven't been registered, during the 7.3.9 installation non-critical errors with deregistration of these files may appear. Ignore them.

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 `IC7310WinAgentClient.zip` file.

3. Copy the IC7310WinAgentClient 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 IC7310WinAgentClient folder and double-click on setupwin32.exe to start the installation program.

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

    c. The next screen displays the License Agreement.

    d. Select the **I accept the terms in the license agreement** option, click **Next**.

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

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

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

    h. 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\7.3.10\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\7.3.10\AvayaAgent\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 the installation is successful, reboot the agent computer.

Avaya Agent installation in silent mode

On the Windows platform, you can also run the IC 7.3.10 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 SP 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 SP 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.

Chapter 4: IC 7.3.10 SP 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: `Start “Avaya IC ORB Service 7.3” from Services console.`
   - Solaris, AIX and Linux: `./icadmin so`.
3. Press **Enter**.

Mandatory Configurations

Following configurations are mandatory to perform so that IC 7.3.10 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

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 several IC releases, Java and Tomcat are upgraded. Therefore all Avaya IC services need to be deleted and re- deployed using config tool and that will ensure that the correct java and tomcat versions are used by the services.

If you are upgrading from release with the same Tomcat and Java as a new one,then you can skip this section

IC Release	New Java version	New Tomcat version
7.3.4	JRE 1.8.0_40 (old 1.6.0_45)	8.0.*
7.3.8	JRE 1.8.0_181 Oracle	8.0.*
7.3.9	JRE 1.8.0_181 Zulu Open JDK	9.0.*
7.3.10	JRE 1.8.0_292 Zulu Open JDK	10.0.4

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”.

Note for Windows Machine: If WebLM is not extracted in `<AVAYA_IC73_HOME>\tomcat\webapps\WebLM` folder then follow below steps before starting tomcat\WebLM service:

a. Create an empty directory ‘WebLM’ folder in `<AVAYA_IC73_HOME>\tomcat\webapps`
b. Unzip the WebLM.war in above mentioned folder.

Steps to be performed on machine where SDK Server is configured

For SDK server, we do NOT have an option to uncheck and check the SDK service in the Configtool and hence we need to recreate the SDK service. The following steps have to be performed for that.

1. Stop SDK service
2. Run config tool.
3. Go to “SDK Server” tab and click on Apply.
4. For more information on starting and stopping SDK server, see IC 7.3 Installation and Configuration guide.

Steps to be performed on machine where Webservices is configured

For Webservices, we do NOT have an option to uncheck and check the Webservice in the Config tool and hence we need to recreate the Web service The following steps has to be performed for that.

1. Stop webservices
2. Make sure following parameters are set in the <AVAYA_IC73_HOME>tomcat/bin/icwebservices.bat (windows) and <AVAYA_IC73_HOME>tomcat/bin/icwebservices.sh (Solaris) :
   a) AVAYA_IC_WEBCLIENT_URL

   b) AVAYA_IC_VESP_JAVAAPPBRIDGE_NAME
3. Remove and re-configure service. For more information on remove and Configure WebService's service, see IC 7.3 Installation and Configuration guide.
4. Start the webservices

For more information on starting and stopping WebServices server, see IC 7.3 Installation and Configuration guide.

Steps to be performed on WebConnector machine:

For WebConnector, we do NOT have an option to uncheck and check the WebConnector in the Configtool and hence we need to recreate the Webconnector. The following steps has to be performed for that

1. Stop AAWC.
2. Remove the `aawcclient.bat` (Windows)/`aawcclient.sh`(Solaris) from `<Avaya_IC73_Home>\bin`
3. Run config tool.
4. Go to "Web Client" tab and click on Apply.
5. Redeploy the newly created `webclient.war` file. For more information, see IC 7.3 Installation and Configuration guide.
6. Start AAWC.

For more information on starting and stopping AAWC, see IC 7.3 Installation and Configuration guide.

Database Configuration

The database can be reconfigured with the following steps:

1. Merge existing customizations, if any, into `ccq_735.adl` and `repository_735.adl`.
2. Rename the ADL files and reconfigure the database.
3. Import new properties. If you are upgrading from IC 7.3.2 or later releases you can skip this step.
4. Restart Directory server.

1. Merge existing customizations in ADL

Note : Repository and ccq files were not modified in 7.3.10 SP hence the file names remain as ccq_735.adl and repository_735.adl . If the upgrade is from 7.3.5 FP or later, then the below steps can be ignored.

Note: To enable OAuth2 feature, you have to customize files manually. Go to "Enhancements in IC 7.3.10 Service Pack: OAuth 2.0 Support" paragraph in this document.

IC 7.3.10 Service Pack contains `ccq_735.adl` and `repository_735.adl` files in `<AVAYA_IC73_HOME>/design/CallCenterQ` and `<AVAYA_IC73_HOME>/design/repository` folders respectively. You must manually merge your customizations into `ccq_735.adl` and `repository_735.adl`.

2. Rename the ADL files and reconfigure the database

Note : If the upgrade is from 7.3.5 FP or later, then the below steps can be ignored

You must perform the below steps irrespective of whether or not the ADLs are customized.

1. Go to `<AVAYA_IC73_HOME>\design\CallCenterQ` folder and take a backup of the existing `ccq.adl.` This is the ADL which was present in the system before the IC 7.3.9 SP was applied. Rename `ccq_735.adl` to `ccq.adl`.

2. Similarly, go to `<AVAYA_IC73_HOME>\design\repository` folder and take a backup of `repository.adl and` rename `repository_735.adl` to `repository.adl`.

3. Reconfigure the database and generate windows applications.

3. Import new properties (TemplateDownload and StatusDownload - Introduced in IC 7.3.2 SP and FilterPoolsByTenant - Introduced in IC 7.3.6 SP)

1. Log on to the IC 7.3.10 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

Seed data has been modified in 7.3.3 FP, 7.3.5 FP, 7.3.6 SP and also in 7.3.7 SP. This section is split in to 4 sections

1) **Seed data for properties introduced in 7.3.3 FP**
2) **Seed data for properties introduced in 7.3.5 FP**
3) **Seed data for properties introduced in 7.3.6 SP**
4) **Seed data for properties introduced in 7.3.7 SP**

Note: If you are upgrading from releses prior to 7.3.3 FP, then all the steps has to be performed.

Seed data for properties introduced in 7.3.3 FP:

Note : If the upgrade is from 7.3.3 FP, then the below steps can be ignored.

To import the new seed data introduced in 7.3.3 FP, perform the following:

For Properties :

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 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
   ```

For RL Manager Table:

1. Open a command prompt and enter `<IC_HOME>\design\CallCenterQ\data`.

2. Open `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 if not present:

   ```
   Table=qem_folder
   ```

4. Comment other #Table entries.

5. Save and close the `seed.cfg` file.

6. Run `import_seed.bat` or on command prompt run following command:

   ```
   ..\..\..\bin\qimport import seed.cfg
   ```

Seed data for properties introduced in 7.3.5 FP :

Note : If the upgrade is from 7.3.5 FP, then the below steps can be ignored.

To import the new seed data for 7.3.5 :

1. Open a command prompt and navigate to IC73_INSTALL_DIR\IC73\design\CallCenterQ\delta.

2. Open migrate_seed_735.cfg in an ASCII editor such as Notepad and verify that the administration login ID and password are correct.

3. Save and close the migrate_seed_735.cfg file.

4. Run migrate_seed_735.bat.

There should be exactly one successful run of the batch file.

Multiple runs will add the same entries multiple times in the affected tables.

In case there are multiple entries accidentally, use these queries to remove the entries (after appropriate database names), and run the batch file again.

```
DELETE FROM [ccq_ic73].[dbo].[w_log_event_master]
     WHERE [event_type]=702
GO

DELETE FROM [ccq_ic73].[dbo].[w_log_event_detail]
      WHERE [event_type]=702
GO
```

5. Restart the servers in the following sequence: DS, Paging Server, WACD.

Seed data for properties introduced in 7.3.6 SP :

Note : If the upgrade is from 7.3.6 SP, then the below steps can be ignored.

To import the new seed data for 7.3.6 :

1. Open a command prompt and navigate to IC73_INSTALL_DIR\IC73\design\CallCenterQ\delta.

2. Open migrate_seed_736.cfg in an ASCII editor such as Notepad and verify that the administration login ID and password are correct.

3. Save and close the migrate_seed_736.cfg file.

4. Run migrate_seed_736.bat.

There should be exactly one successful run of the batch file.

Multiple runs will add the same entries multiple times in the affected tables.

In case there are multiple entries accidentally, use these queries to remove the entries (after appropriate database names), and run the batch file again.

```
DELETE FROM [ccq].[dbo].[w_log_event_detail]
      WHERE [event_type]='82'and [key_name]='tenant_id'
GO
```

5. Restart the servers in the following sequence: WACD, ICEmail

Seed data for properties introduced in 7.3.7 SP :

To import the new seed data for 7.3.7 :

1. Open a command prompt and navigate to IC73_INSTALL_DIR\IC73\design\CallCenterQ\delta.

2. Open migrate_seed_737.cfg in an ASCII editor such as Notepad and verify that the administration login ID and password are correct.

3. Save and close the migrate_seed_737.cfg file.

4. Run migrate_seed_737.bat.

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.

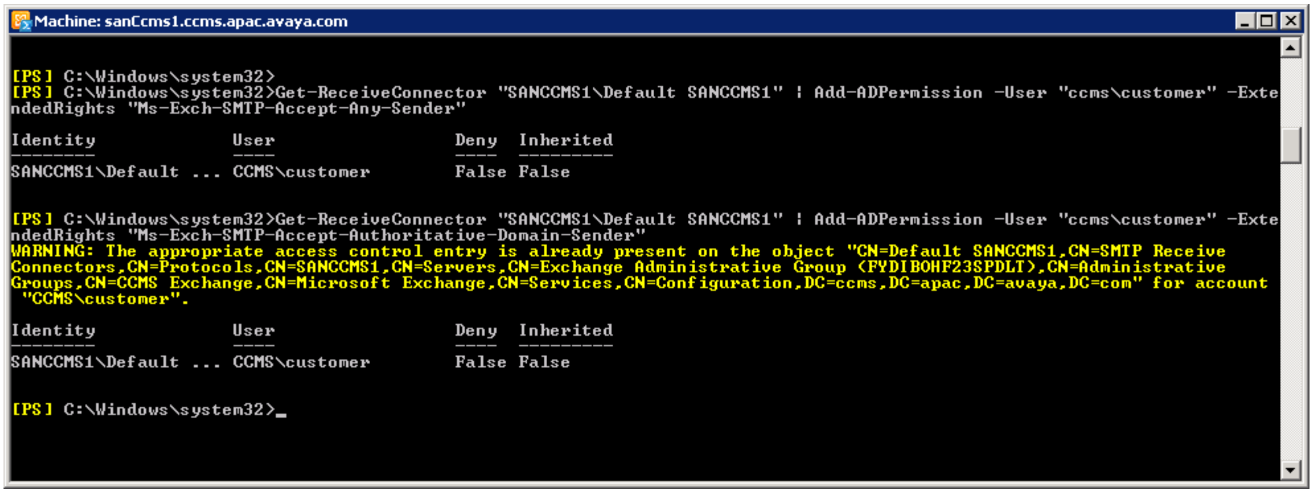
```
Get-ReceiveConnector "SANCCMS1\Default SANCCMS1" | Add-ADPermission -User
"ccms\customer" -ExtendedRights "Ms-Exch-SMTP-Accept-Any-Sender"
```

```
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
```

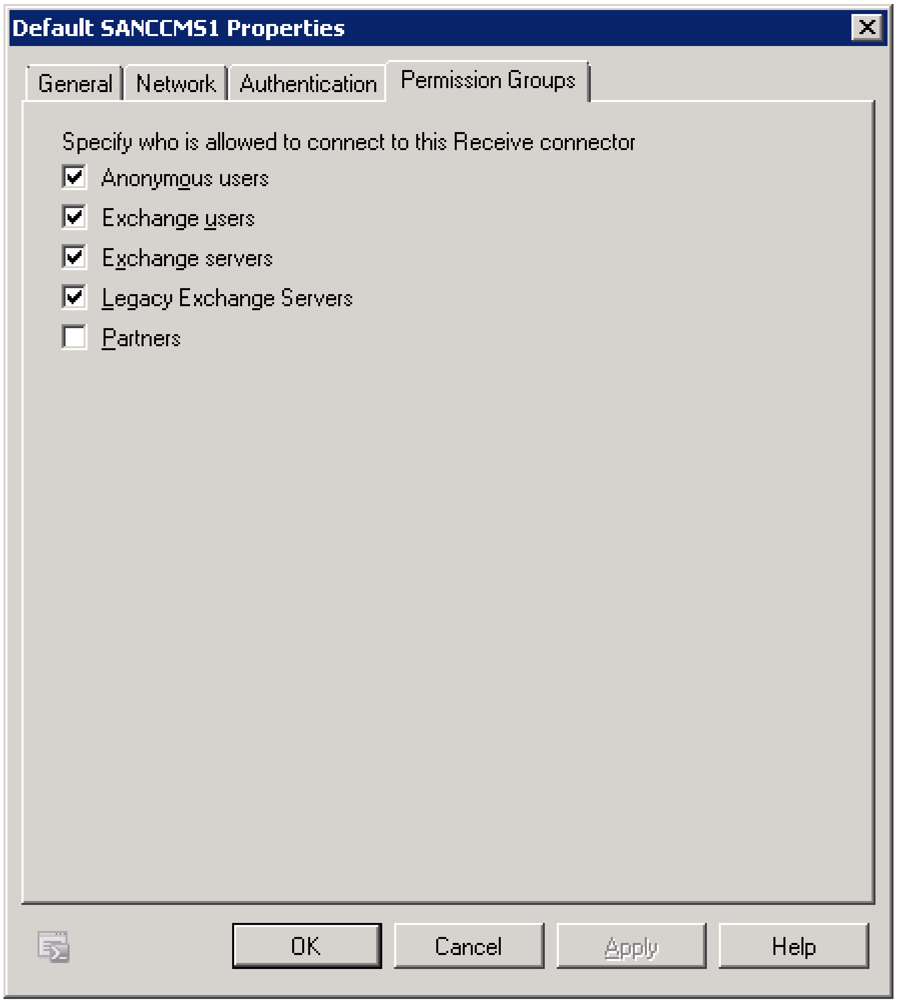
Send an email from the website and check the received connector name handling the email send by the website (IP of the computer hosting the website).



```
[PS] C:\Windows\system32>
[PS] C:\Windows\system32>Get-ReceiveConnector "SANCCMS1\Default SANCCMS1" | Add-ADPermission -User "ccms\customer" -Exte
ndedRights "Ms-Exch-SMTP-Accept-Any-Sender"

Identity              User                  Deny  Inherited
--------              ----                  ----  ---------
SANCCMS1\Default ...  CCMS\customer         False False


[PS] C:\Windows\system32>Get-ReceiveConnector "SANCCMS1\Default SANCCMS1" | Add-ADPermission -User "ccms\customer" -Exte
ndedRights "Ms-Exch-SMTP-Accept-Authoritative-Domain-Sender"
WARNING: The appropriate access control entry is already present on the object "CN=Default SANCCMS1,CN=SMTP Receive
Connectors,CN=Protocols,CN=SANCCMS1,CN=Servers,CN=Exchange Administrative Group (FYDIBOHF23SPDLT),CN=Administrative
Groups,CN=CCMS Exchange,CN=Microsoft Exchange,CN=Services,CN=Configuration,DC=ccms,DC=apac,DC=avaya,DC=com" for account
 "CCMS\customer".

Identity              User                  Deny  Inherited
--------              ----                  ----  ---------
SANCCMS1\Default ...  CCMS\customer         False False


[PS] C:\Windows\system32>_
```

c. Restart the Microsoft Exchange Transport service.

d. Make sure the Receive connector has checkbox enabled for **Anonymous users** under the **Permission Group** tab.



Specify who is allowed to connect to this Receive connector

☑ Anonymous users

☑ Exchange users

☑ Exchange servers

☑ Legacy Exchange Servers

□ Partners

Exchange 2013 and 2016 configuration changes

Exchange server 2013 and 2016 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 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.

1. Perform the following configuration steps to replace the files:

2. Extract `%AVAYA_IC73_HOME%\sdk\server\icsdk.war` on local computer, for example: `c:\icsdkextract\`. Avoid extracting the war in `sdk\server` folder, as it might overwrite existing customizations, if any.

3. Manually copy all jar files from `WEB-INF\lib\` of the above extracted folder, for example: `c:\icsdkextract\ WEB-INF\lib` to `%AVAYA_IC73_HOME%\sdk\server\icsdk\WEB-INF\lib\`.

Upgrading IC SDK Client

As part of the SP upgrade, all the client files would be copied by the installer in the %AVAYA_IC73_HOME%\sdk\design\java\lib path and %AVAYA_IC73_HOME% \sdk\design\dotnet\lib in the SDK Server machine. Ensure that the custom clients built using client SDK APIs are compiled using the latest .jars or dlls from the above location.

Upgrading WebLM to 8.0.1 (acceptable for 8.1.3)

The upgrade steps mentioned below are specific to upgrade of WebLM server from release 7.0.1 to 8.0.1. Note: This new version of WebLM requires Tomcat to be upgraded to release 9.0.12.

An assumption is made that the user has WebLM running. There is also some configuration that the user has done (for the installed product) that user would like to retain after re-installing the WebLM.

The set of files/folders that user might want to retain are shown in the table below

File/Folder	**File location**	**Required**	**Description**
Product_folder – Folder	<tomcat_installation_dir>/webapps/WebLM/data/	Yes	The product folder that contains the configuration files.
weblmserver.properties	<tomcat_installation_dir>/webapps/WebLM/data/	Yes, if some default settings have been modified.	This files contains some WebLM specific configuration properties.
log4j.properties	<tomcat_installation_dir>/webapps/WebLM/WEB-INF/classes	Yes, if some log4j properties have been modified.	This file contains WebLM logging related configuration properties.

Note:
It is not possible to restore Users.xml in weblm 8.0.1 as since weblm 7.1 due to security password encryption has been changed and later on the digital signature.

Following are the set of generic steps one needs to follow to upgrade WebLM:

1. Stop Tomcat server.
2. Before uninstalling/removing WebLM, back up the set of files as described in the table above.
3. Delete WebLM folder recursively from <tomcat_installation_dir>/webapps. Delete the WebLM application file WebLM.war (if present) from <tomcat_installation_dir>/webapps.
4. Re-install the new version of WebLM. Refer section Installation and Configuration to Configuring the WebLM.
5. Before restoring the above set of files, ensure that Tomcat is stopped.
6. Restore/Overwrite the above set of files in the respective file/folder location.
7. WebLM 8.0.1 requires that CATALINA_HOME environment variable to be set:
   Note: CATALINA_HOME = %AVAYA_IC73_HOME% \tomcat
8. Start Tomcat & access WebLM.

Note: After upgrading WebLM from 7.0.1 to 8.0.1 version, HostID will be changed. You have to request a replacement license. This request is described in “AIC Installation Planning and Prerequisites guide” document, chapter 8:”Interaction Center Licensing”, section “Requesting a replacement license file”, https://downloads.avaya.com/css/P8/documents/100159305

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 7.3.10 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 7.3.10 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.

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]**
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	A popup option would be displayed asking the user	If the user presses the Ok button after the session

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]
	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`.	if he needs to escalate the chat. `OK`: Will escalate the chat again. **Cancel**: Will prevent the chat escalation.	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.

The following procedure may need to be executed by a user with Administrator rights on all IC core server systems in cases some issues with Chat/Email transcripts are observed (for example, transcripts are not sent to the customer's e-mail or can't be viewed on the Web Administration page) or ICEmail or Poller servers cannot start:

1. Remove "%AVAYA_IC73_HOME%\Java\bin\server" from the path system variable
2. Execute the following commands using EnvironmentUpdate-75.jar
   java.exe -jar .\EnvironmentUpdate-75.jar bin\msal4jspec-1.0.jar Java\jar\mail.jar etc Java\jar\mail.jar etc
   java.exe -jar .\EnvironmentUpdate-75.jar bin\msal4jspec-1.0.lib\javax.mail-1.6.1.jar none Java\jar\mail.jar none Java\jar\mail.jar
3. Restart the core machine after execution.

Email accounts for chat transcript in CS Portal (Introduced in IC 7.3.7 SP)

The CS Portal / ICM uses first email address entered into the IC Manager for a particular tenant as an email address to send a chat transcript. If this account is disabled, the account configured next is treated as the default account, and this process continues till an email account that is not disabled is found.

To configure CS Portal / ICM to use a specific email address follow the steps below. Please note, the email address **MUST** be configured in IC Manager.

Perform the following steps on the CS Portal redirector server:

1. Open IIS
2. Click the server name and select Stop the IIS server

Perform the following steps on the CS Portal server:

1. Open the Windows Services
2. Stop CS Portal Service
3. Stop ICM Service
4. Navigate to the tomcat\work folder. Delete the Catalina folder.

Perform the following steps on the CS Portal redirector server:

1. Navigate to the CSPortal\Refimplementation\js folder
2. Make a copy of the app.js file
3. Open the app.js file to edit
4. Scroll down to the “function requestChat(option)”
5. There is a series of “requestObj”. You will add requestObj.aicaddress = ' icemail@test.com';
6. Here is an example of the OOTB code with the additional email line.

```
function requestChat(option) {

    var requestObj = {};

    if (option && option.auto == true) {

        //Auto-Login

        requestObj.displayname  = "Guest";

        requestObj.question = defaultQuestion;

    } else {

        requestObj.displayname = $('#fbLiveChatName').val();

        requestObj.sendemailto = $('#fbLiveChatEmailId').val();
        requestObj.sendtranscript = 
document.getElementById('fbEmailSendTranscript').checked; //true or false

        requestObj.question = $('#fbLiveChatQuestion').val();

        requestObj.aicaddress = ' icemail@test.com';

  }
```

7. Save the file
8. Start IIS

Perform the following steps on CS Portal server:

1. Start ICM Service
2. Start CS Portal Service

Perform the following steps on client machine:

3. Open Browser
4. Clear Browser history
5. Complete a test chat with a transcript request through the internal URL to the server you have changed

With the "aicaddress" parameter it is possible to control which "From/Reply-To" email address to be used instead of email address configured in the first email account. Also the corresponding outgoing SMTP connection is used.

Local timestamps in the chat transcript (Introduced in IC 7.3.7 SP)

The chat transcripts were previously stored in UTC format in the DB. There were requirements from the customers to store the transcripts in Local time format.

From Release 7.3.7, IC can be configured to use local time stamp for the transcripts in the DB. A new configuration has been added and by default this configuration is turned off (UTC format would be used).

To configure local timestamps in the chat transcripts perform the following:

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

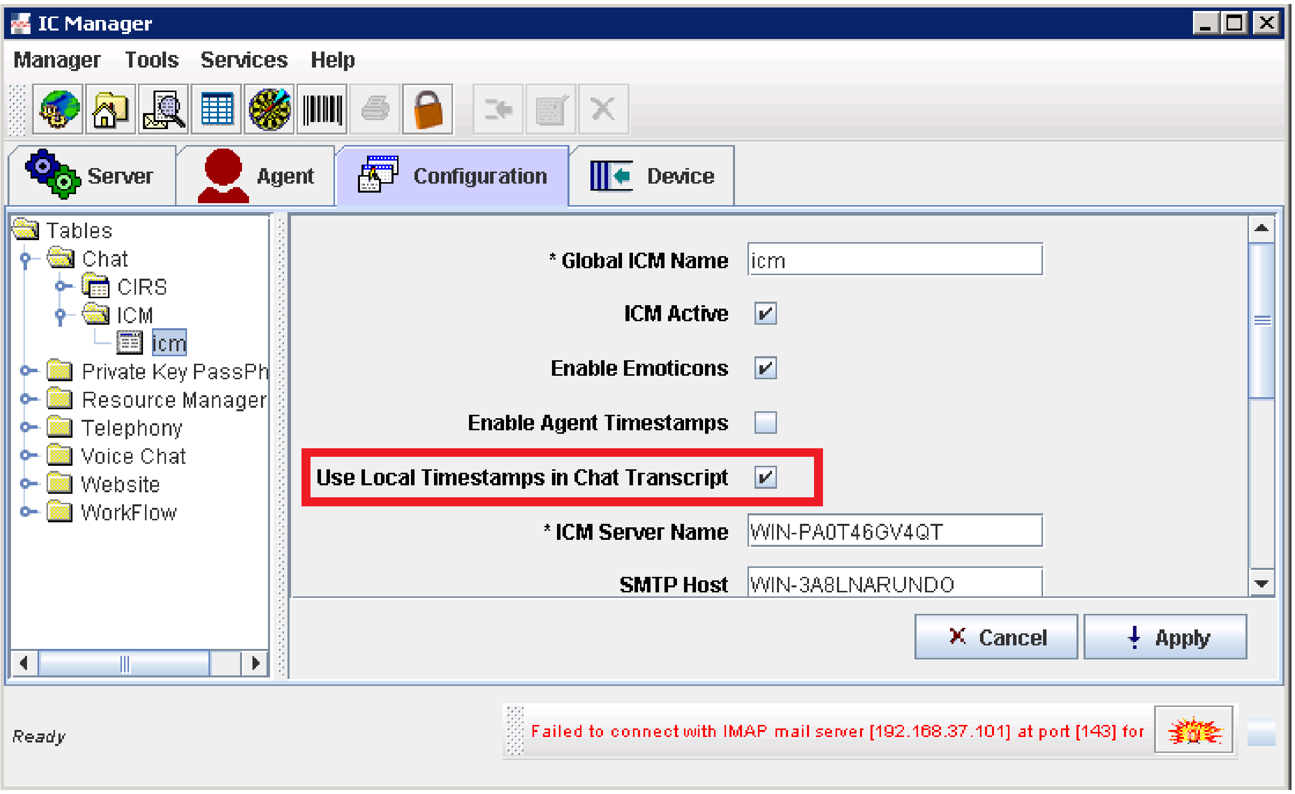
2. After successful import re-launch IC Manager.

3. Go to the IC Manager Configuration tab.

4. A new check box, “Use Local Timestamps in Chat Transcript”, is present.

5. Select “Use Local Timestamps in Chat Transcript”.

6. Restart the ICM service.



* Global ICM Name: icm

ICM Active ☑

Enable Emoticons ☑

Enable Agent Timestamps ☐

Use Local Timestamps in Chat Transcript ☑

* ICM Server Name: WIN-PA0T46GV4QT

SMTP Host: WIN-3A8LNARUNDO

Ready

Failed to connect with IMAP mail server [192.168.37.101] at port [143] for

Searching For Emails in agent clients with From address (Introduced in IC 7.3.6 SP)

When an agent searches for emails using the customer’s From field address, by default the LIKE is used in the SQL query to retrieve the messages. This could result in messages being listed where the From is not exactly the address/parameter provided in the query.

To search for messages where an exact match of the From address is required, then configure the following on the Configuration tab of the ICEmail server. Once you have completed the configuration you must restart the ICEmail server.

FromEmailExact as **1**

The above will retrieve messages where the From field is an exact match of the parameter passed in the search field.

e.g. There are 2 emails having From as cust1@xyz.com, and another 2 emails having From as 2cust@test.com.

If **FromEmailExact** is not configured (default; or != 1), then in agent client a search of customer email address using *cust* will fetch all 4 messages.

If **FromEmailExact=1** is configured, then a search of customer email address using *cust* will not fetch any emails.

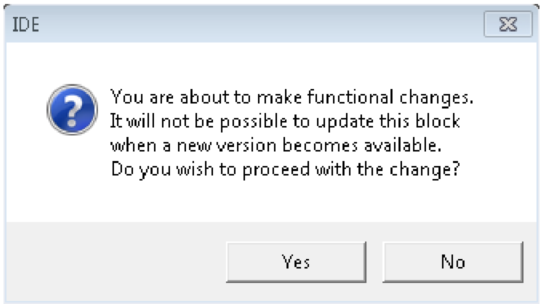
When cust1@test.com is used then both emails will be fetched (provided they are in the timeline parameter).

Similarly, when 2cust@test.com is used then other 2 emails will be fetched (provided they are in the timeline parameter).

“Forward Original” feature related configuration in Email Workflow (Introduced in IC 7.3.5 FP)

To Address routing of “Forward Original” email (performed by Agent using AARC) to correct queue/workgroup, OOTB “Route” block of “analyzeca” and “analyzenoca” email workflows are modified. Without this change, “Forward Original” email will route to previous agent. You can merge the “Route” block script in your existing “Route” block script. Follow the below steps to make/merge the changes in “Route” block –

1. On “Design And Admin” machine, take the backup of Email flows. Flows are located at location <AVAYA_IC73_HOME>\ design\IC\Flows\Avaya\ICEmail
2. Open WorkFlow Designer and then open project from <AVAYA_IC73_HOME>\ design\IC\Flows\Avaya\ICEmail
3. Select “analyzenoca” flow.
4. Select “Get EDU Values” block
5. In Property Sheet, select “Basic” tab
6. Declare following field/target values
   a) Field_XX/Target_XX = parentmsgid/$parentmsgid
   b) Field_XX/Target_XX = currentemail.header.XWF_ReplyType/$replytype
7. Save the changes
8. Now select “Route” block. There are TWO “Route” blocks in OOTB flow. You should choose the “Route” block which would hit when “EmailType=NOR” condition fails.
9. In Property Sheet, select “Advance” tab and click on “Route”. It will display following message



You are about to make functional changes.
It will not be possible to update this block
when a new version becomes available.
Do you wish to proceed with the change?

10. Select “Yes”.

11. IC Script Editor will open

12. Declare following variable at top of the block

```
Dim bSetPrefAgent as boolean
Dim iSession as AppSession
Dim iNetwork as DBNetwork
Dim iTable as DBTable
Dim sParentEduId as String
Dim sParentFrAddr as String
Dim iRecord as DBRecord
```

13. After line “`' handle routeresponsetoagent here`” Add following code

```
' Handling for Forward Original Scenario
' cond 1 - parent's EduId is allocated to more than one message ids
' cond 2 - parent's from address should not be the polling address
' If (cond 1) and (cond 2) then this is "Forward Original" email.
' if "Forward Original" then do not set the preferred agent.

bSetPrefAgent = true
If Script.variable.replytype = "FWD" Then
      ' Check cond 1
      Set iSession = GetSession()
      Set iNetwork = iSession.GetNetwork()
      Set iTable = iNetwork.GetTable("qem_message")

      iTable.QBEClear
      iTable.QBESetValue "pkey", "=" & Script.variable.parentmsgid
      iTable.Search

      if iTable.RecordCount = 1 Then
            Set iRecord = iTable.GetRecord(0)
            sParentEduId = iRecord.GetValue("du_recovery")
            sParentFrAddr = iRecord.GetValue("fromaddress")

            iTable.QBEClear
            iTable.QBESetValue "du_recovery", "=" & sParentEduId
            iTable.Search
```

```
        if iTable.RecordCount > 1 Then
            ' Check cond 2
            Set iSession = GetSession()
            Set iNetwork = iSession.GetNetwork()
            Set iTable = iNetwork.GetTable("qem_mailaccount")

            iTable.QBEClear
            iTable.QBESetValue "mailbox", "=" & sParentFrAddr
            iTable.Search

            if iTable.RecordCount = 0 Then
                bSetPrefAgent = false
            End if
        End if
    End if
End if
```

14. Then modify following condition

```
if {_#RouteResponseToIntendedAgent} = "true" AND _
    Script.variable.previouslyhandled = "1" then
    Script.variable.routeresponsetoagent = 1
else
    Script.variable.routeresponsetoagent = 0
end if
```

15. To

```
if bSetPrefAgent = true AND _
    {_#RouteResponseToIntendedAgent} = "true" AND _
    Script.variable.previouslyhandled = "1" then
    Script.variable.routeresponsetoagent = 1
else
    Script.variable.routeresponsetoagent = 0
end if
```

16. Compile the script to make sure there are not errors.

17. Click **OK**.

18. Save the changes

19. Build the Flow Set

20. Stop and Start the WorkFlow Server which is responsible for executing “analyzenoca” flow

21. Perform the same steps if you want to do similar changes in “analyzeca” flow.

Configuration related to WSCallback server (Introduced in IC 7.3.5 FP)

Select the WSCallback Server tab and right click for advanced configurations.

Add the value as relevant to the environment.

Wait time For Cache Ready - [Default value : 2000ms , min : 2000ms , max : 8000ms]

Configuration related to ICEmail server (Introduced in IC 7.3.5 FP)

This configuration is mostly relevant if the property Agent\Desktop\WrapupEnabled is set to false.

A parameter ‘TerminateEDUDelay’ has been introduced to induce a delay between the time an email contact is wrapped and before its Eduid is terminated. The default value is 7 seconds. To change the value follow the steps mentioned below:

1. Edit the ICEmail server. Go to the Configuration tab.

2. Add the below Key-Value pair:

   Key: TerminateEDUDelay

   Value: 7 (Time in seconds)

Note: The recommended value is 7 seconds, setting the parameter to a very low value might cause issues while creating Hub Eduids for email replies.

Configuration related to Chat Blind Transfer (Introduced in IC 7.3.5 FP)

Declare a property AllowBlindTransfer as integer in IC manager.

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/WAC**.
4. Add following property under this **AllowBlindTransfer (Datatype - integer)**.
5. Click **OK**.
6. Go to **Tools > Groups** and add the above properties under **Agent/Desktop/WAC**.

Use the following value to select the type of chat transfer

Value	Description
1	Default value. Transfer will be consultative transfer. Blind transfer option will be disabled.
2	Agent can only do blind transfer to Queues. WebAgent will enable only Blind transfer option. Agent Tab in UAD will be disabled.
3	Agent can perform both the blind and consultative transfer. WebAgent will display both the menu options i.e Blind Transfer and Transfer(Consultative)

ASGPlugin Keys Update for Remote Access (Introduced in IC 7.3.5 FP)

Access Security Gateway keys update. In keeping with NIST guidelines and industry best practices, Avaya is rotating the security keys associated with remote maintenance access through the Access Security Gateway (ASG).

Pre-requisites:

- This change is applicable to ONLY to Windows Server, Windows Design & Admin, and Windows Web Connector systems, where *ASG is available and enabled*.
- A new Authentication File is downloaded from Remote Feature Activation website https://rfa.avaya.com
- If ASG is disabled before or after IC 7.3.6 SP installation then only perform steps 1 & 2 and no need to perform steps from 3 to 5.

Steps to update keys:

1. Login as an Administrator
2. Go to "**C:\Program Files\Avaya\ASGPlugin**" folder on the system and remove the default Authentication File "**ASGPluginAFSFile.xml**"
3. Copy the newly downloaded Authentication File to "**ASGPlugin**" folder
4. Ensure all copies of the new authentication file are destroyed except the one in the protected "**ASGPlugin**" folder.
5. Start the "**ASG Service**" from Services Management Console, if not started already.

Configuring Estimated Wait Time (EWT) for Non-BA Chat (Introduced in IC 7.3.5 FP)

Estimated Wait Time feature for Non-BA Chat is by default disabled. To enable the feature, the following configurations are required in WACD Server and CSPortal. This is only supported with CSPortal.

WACD

ewtFlavor

This configuration sets the version of the EWT feature.
There are two flavors.
ewtFlavor=1 which gives the exact EWT
ewtFlavor=2 This is the optimized version calculation, which provides for a “far end” estimate.
For 7.3.5, only ewtFlavor=2 is supported.
By “far end”, it means that the optimized version rounds off the chat task position in the queue, and time calculation, towards the larger side.

ewtAhtSeed

This is to configure the start “seed” value in seconds for the Agent Average Handling Time (AAHT).
This value will be used for the first time in EWT calculation on every WACD restart.
This is an optional configuration for non-BA Chat EWT.
Default value: 60 seconds

To set the above configuration parameters:

- Login to IC Manager with Admin privileges.
- Edit the **WACD** server
- Go to the **Configuration** tab.
- Click the **New** to open the 'CTI Type Editor'.
- Provide the values for this new couple as:

Name	**Value**
ewtFlavor	2
ewtAhtSeed	**120**

- Click OK.
- Click **OK** in **WACD** Editor.
- Restart the **WACD** in IC Manager.

CSPortal

If the **aic_chat.js** file deployed in CSPortal Web API client is customized, then the changes has to merge with the aic_chat.js that comes with IC7.3.5 installer.

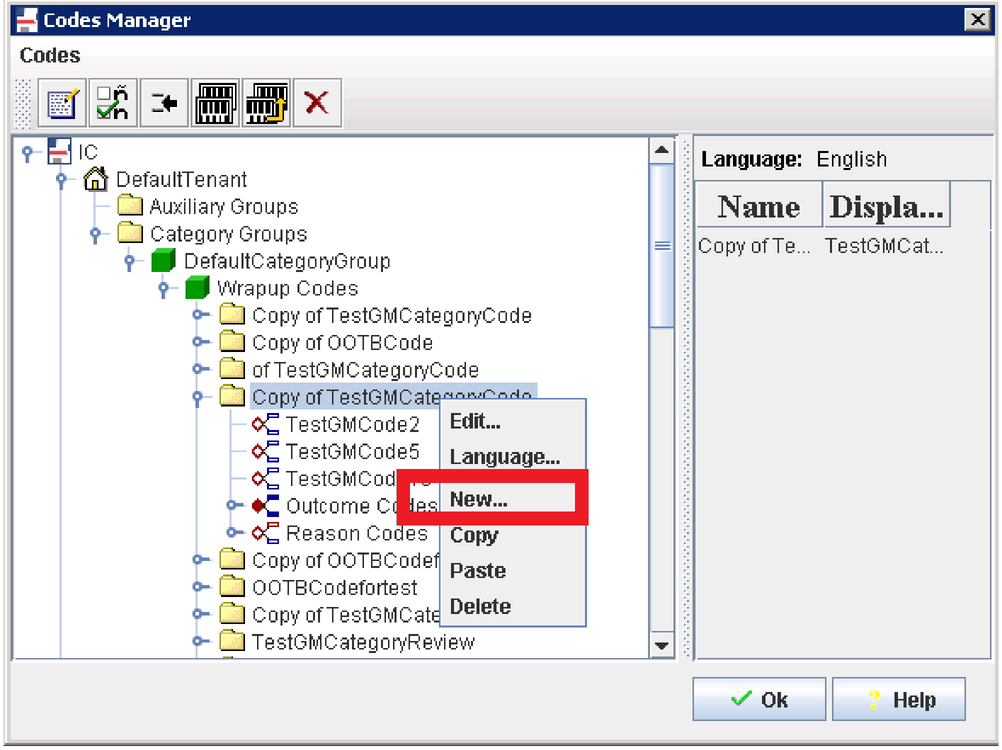
The **aic_chat.js** should be copied on the machine where CSPortal Web API client is deployed.

The file **aic_chat.js** is located in <AVAYA_IC73_HOME>\design\csportalclient\sdk\js. Refer to "CSPortal WebAPI client side deployment" section in Install and Configuration guide.

Configuring variable number of Wrapup code types (Introduced in IC 7.3.4 SP)

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.



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.

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.

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. Log in 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 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`, `CtiObjectDoesNotExistException`, `CtiResourceException`. In case of network failure between RLManager and ICEmail server, RLManager receives CTI exceptions.

Sr. No.	Configuration parameter	Default value	Mandatory?	Description
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 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. Its 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:

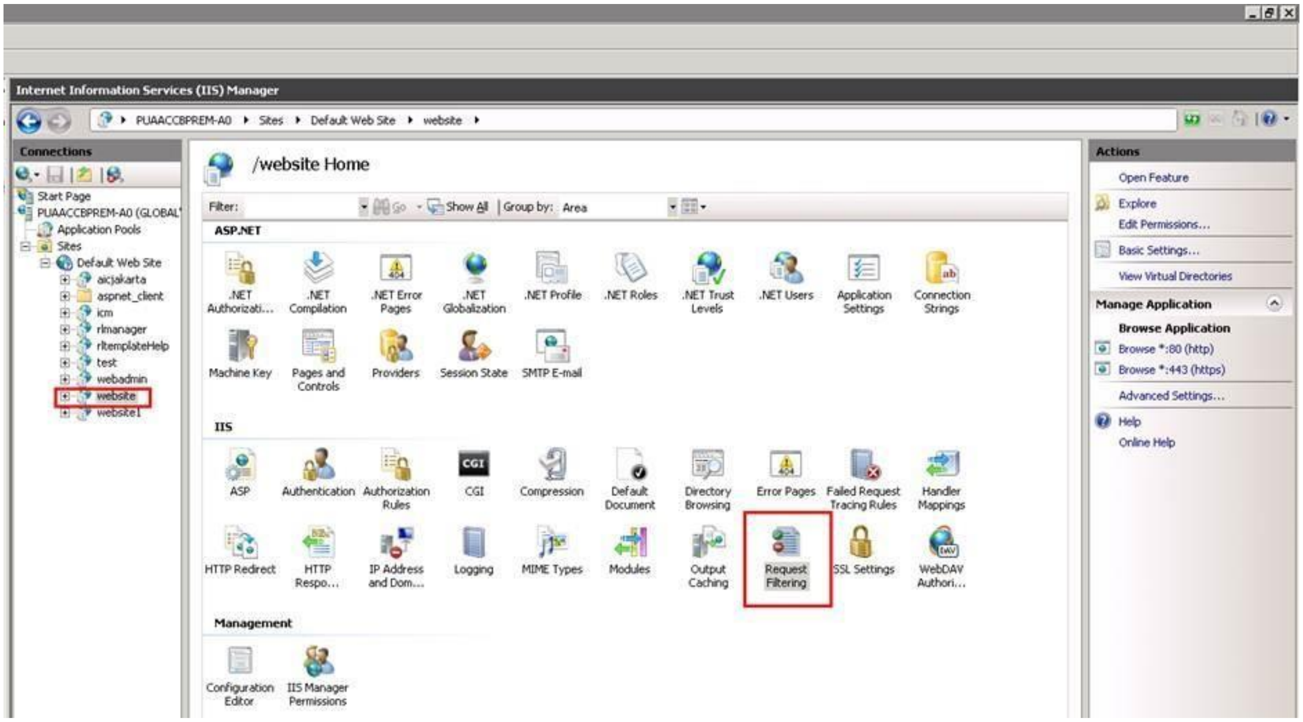
- Always deploy Public and Administration website on separate servers.
- Have the server hosting the Administration website behind the firewall.
- Always enable HTTPS and disable HTTP for webserver and the Tomcat application.
- Turn off folder browsing for the website on the webserver.
- Turn off Anonymous access to website related files/folders by the webserver application.

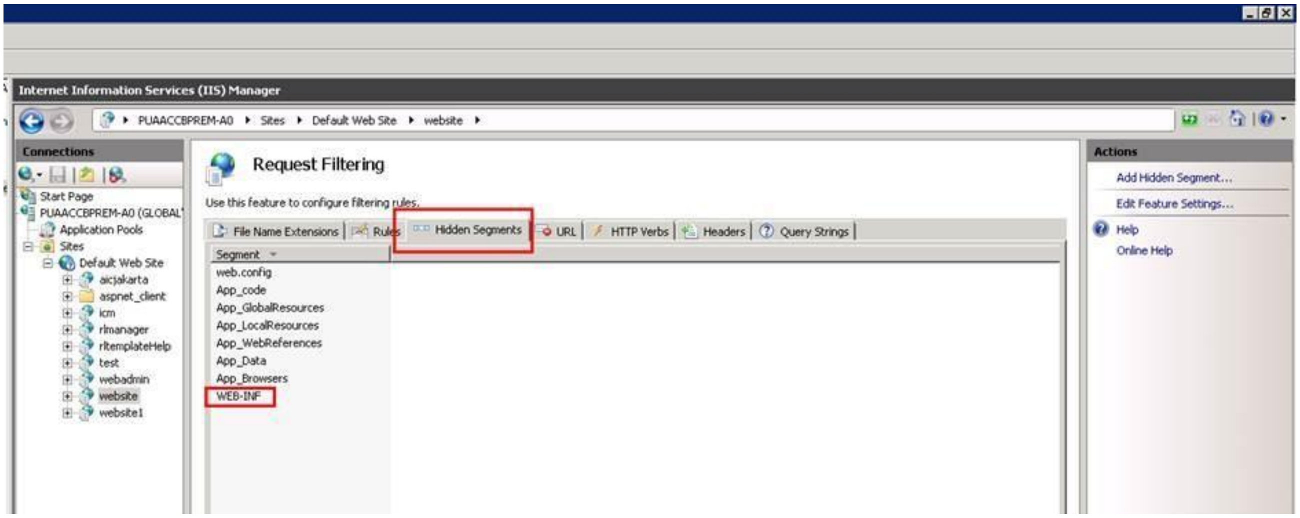
Note: Recommendations #1 & 2 helps secure IC website against the following vulnerability:

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

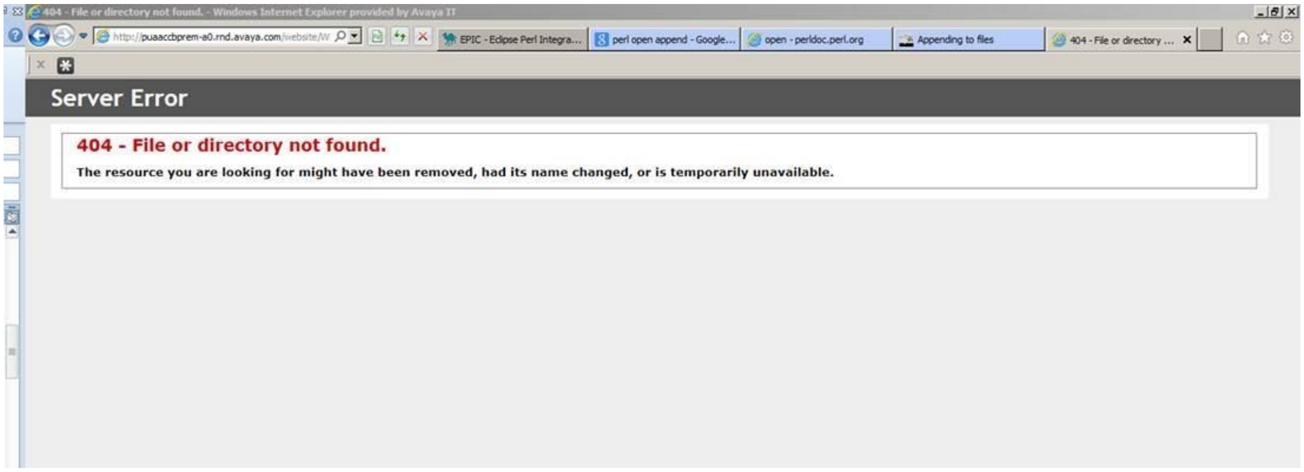
The changes are related to have IIS deny requests containing sensitive URLs. For example, by default IIS restricts all requests trying to serve content from the 'bin' folder. However, as WEB-INF is a Tomcat thingy, we will need to specifically tell IIS to not to serve these URLs. Here are screenshots for the same:





Use this feature to configure filtering rules.

Segment
web.config
App_code
App_GlobalResources
App_LocalResources
App_WebReferences
App_Data
App_Browsers
WEB-INF


404 - File or directory not found. - Windows Internet Explorer provided by Avaya IT
http://puaaccbprem-a0.rnd.avaya.com/website/W
EPIC - Eclipse Perl Integra...
perl open append - Google...
open - perldoc.perl.org
Appending to files
404 - File or directory ...

Server Error

404 - File or directory not found.

The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

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 anykey 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 7.3.2 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
```

Chapter 5: Uninstall program

The Avaya IC 7.3.10 installation program installs an uninstall program that can remove the files from the IC 7.3.10 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 SP 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 SP to restore the system to its original state.

- The uninstaller is not created:

  When the uninstaller is not created, it implies that the SP 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 7.3.10 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 7.3.10

Perform the following steps on a system from where you want to uninstall IC 7.3.10 files:

1. Navigate to the following folder:
   - Windows: `...\IC73\ICServicePacks\7.3.9\<FolderNameOfComponent>\Record\`
   -
2. Start the Uninstall program:

Windows

Double-click the uninstall7.3.10.bat file.

Solaris, AIX (server only) and Linux (server only)

1. At the command prompt, type: `./uninstall7.3.8.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 7.3.10 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\7.3.10\<FolderNameOfComponent>\Record`
Solaris and AIX	`.../IC73/ICServicePacks/7.3.8/<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	`uninstall7.3.10.bat -silent`
Solaris and AIX	`./uninstall7.3.8.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 help files are continue to be part of the IC7.3.10 SP installer and the installation would take of updating the help files.

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

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.

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:

- IC7310WinServer.zip

  This package contains the changed help files for the following IC server components:

  - Business advocate

  - Templatemanager
  - Webservices

- IC7310WinAdmin.zip

  This package contains the changed help files for IC Admin components:

  - Config accelerator (CA)
  - Database designer
  - IC Manager
  - Report Wizard
  - Workflowdesigner

- IC738SolServer.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 IC7310WinAdmin package.
4. From the extracted IC7310Admin 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 IC7310WinServer package.
4. From the extracted IC7310WinServer 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 IC738SolServer package.
4. From the extracted IC738SolServer 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

Chapter 7: Technical Support

If you experience trouble with IC 7.3.10, 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: Service 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/.

Chapter 9: Customer found defects, known issues and workarounds, troubleshooting

For information on known issues and troubleshooting included in Avaya Interaction Center 7.3.**10** 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/.