Avaya Interaction Center

Release Notes

Release 7.3.x

July 7, 2014

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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its 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 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 its hardware and Software ("Product(s)"). 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: http://support.avaya.com

Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, http://support.avaya.com/LicenseInfo/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER; 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. "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.

License type(s)

Designated System(s) License (DS). End User may install and use each copy 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, 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.

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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products". 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 (in the event the applicable Documentation permits installation on non-Avaya equipment) 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, or hardware provided by Avaya. All content on this site, the documentation 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

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: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation 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, and “Linux” is a registered trademark of Linus Torvalds.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support website:

http://support.avaya.com

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product

For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support

Contents

Introduction

The Avaya Interaction Center 7.3.2 Release Notes provides information on installation, configuration, and uninstallation.

This document provides the latest information to supplement Interaction Center software and documentation. For updated documentation, product support notices, and service pack information, visit the Avaya Support Center website at http://support.avaya.com.

Overview

The Avaya Interaction Center (IC) software updates are distributed in service packs. The Avaya Interaction Center (IC) 7.3.2 Feature Pack (**IC Scripts customization merges**) is the second release on top of IC 7.3. This FP is cumulative release which also includes all the fixes from IC 7.3.1 Service Pack. These software updates correct issues and add features not included in the original release of the IC 7.3 system.

Avaya recommends that all IC 7.3 customers update to the 7.3.2 FP level to ensure you have a complete set of fixes. IC 7.3.2 does not include a redelivery of the entire IC product. The IC 7.3.2 FP can be installed on IC 7.3. Follow the instructions in the Release Notes when installing and configuring the IC 7.3.2 Service Pack. Information, such as known defects and defects fixed in this release, and solutions for some known issues, which may 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 their versions are included in the document titled: *FP file list 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 IC 7.3 continue to be in use, unless mentioned otherwise in the Release Notes.

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 FP easily installs all the fixes in the IC 7.3.2 FP.

For additional IC 7.3 documentation information, refer to:

- Interaction Center (IC) 7.3 Product Documentation
- Interaction Center (IC) 7.3 Release Notes
- Avaya IC for Siebel 7 and 8 Integration Guide

Supported new features and configurations

IC supports the following software features and configurations:

Feature/Configurations	IC 7.3	IC 7.3.1	IC 7.3.2
HTML Editor Replacement for Rich Client.	✓	✓	✓
Time in Email Template enhanced to support 24-hour or 12-hour format.	✓	✓	✓
Support for Siebel 7.8.2.13.	✓	✓	✓
SNMP-MIB Enhancement for different OIDs in Traps based on priority.	✓	✓	✓
Ability to enter Email display name in IC Manager.	✓	✓	✓

Feature/Configurations	IC 7.3	IC 7.3.1	IC 7.3.2
Options to set column width, size and location of chat task list in IC agent.	✓	✓	✓
Service Class OWT data in OA reports.	✓	✓	✓
Workflow Server enhanced to handle large number of Workflow channel assignments.	✓	✓	✓
Chat Typing Status Support.	✓	✓	✓
Workflow Server Modification for Dynamic Queue Contact Entry.	✓	✓	✓
Synchronization between Siebel toolbar and Hard phone.	✓	✓	✓
WebAdmin Page Cancel Task with Specified Status.	✓	✓	✓
TSA Server enhanced for Extended UUI Data Support.	✓	✓	✓
Support for IE8 on AAWC.	✓	✓	✓
Restrict the retries by WACD on requesting the WAA to qualify a task when no agent is logged into IC.	✓	✓	✓
Enhanced ASIS to read IC group properties without restart.	✓	✓	✓
Adding UUID and ALIAS of TS in EDU for IVR application.	✓	✓	✓
HttpVOX and VOX support TS.TransferEX method.	✓	✓	✓
VOX Server to handle extension numbers in excess of 2^31.	✓	✓	✓
Monitoring IVR extension using *v assignment.	✓	✓	✓
Indication by WACD about invalid email requalification attempts.	✓	✓	✓

Feature/Configurations	IC 7.3	IC 7.3.1	IC 7.3.2
Disable 'Ready/NotReady' button if agent has not logged into any channel for IC-Siebel.	✓	✓	✓
LDAP integration with Avaya Interaction Center.	✓	✓	✓
SSL Enabled communication between HTTPConnector Server and Dialog Designer 5.1.	✓	✓	✓
Windows 7 support for Avaya Agents and Admin.	✓	✓	✓
Deploying Avaya Rich Client on Citrix XenApp 6.0 on Windows 2008 R2.	✓	✓	✓
Performance gains in SDK WebServices using DS Authentication-Only API over full DS Login.	✓	✓	✓
Support for Microsoft Windows 2008 Server R2 (x64) (Enterprise Edition*)**.	✓	✓	✓
Support for Microsoft SQL Server 2008 (v10.50.1600.1*)**.	✓	✓	✓
Support for hosting IC website using IIS 7.0 on Windows 2008 R2.	✓	✓	✓
Support for hosting IC website using IBM HTTP Server 7.x on AIX 6.1.	✓	✓	✓
Support for deployment of IC on VMWare 4.0.	✓	✓	✓
Oracle Database 11g Client Release 11.2.0.1.0*.	✓	✓	✓
Added Hyperlink button in the HTML toolbar for HTML Editor (only) in Rich Client.	✓	✓	✓
Windows 7, 32-bit Support.	✓	✓	✓
Windows 7, 64-bit Support**.	✓	✓	✓

Feature/Configurations	IC 7.3	IC 7.3.1	IC 7.3.2
Siebel CRM 8.1.1.x support.	✓	✓	✓
Support for Oracle Database Client Release 11.0.2.1.0 on Windows 2008, 64-bit.	✓	✓	✓
Web chat UI and API			✓
Security Enhancements			✓
LDAP authentication support for Admin Website and RL Manager			✓
Selective download of Templates based on Admin configuration			✓
Secured authentication using ASG (Access Security Gateway)			✓
IE 9/10 Support for AAWC, AARC and admin components			✓
JRE and Tomcat Upgrade JRE: Windows/Solaris: 1.6.0_10 to 1.6.0_45 AIX: 1.6.0 SR3 to 1.6.0 SR15 Tomcat: 6.0.14 to 6.0.37			✓
SIP end point support			✓
WebLM 6.3.4 Upgrade			✓
Ephox Html Editor upgrade Editor Editlive is upgraded from 7.5.2.106 to 9.0.0.98			✓
Enhanced Email Migration Tool***			✓
Password encryption when login request is sent to RL Manager			✓
Support for adding multiple attachments into an email			✓

Feature/Configurations	IC 7.3	IC 7.3.1	IC 7.3.2
Reporting provision for RONA exit reason: For RONAed calls exit_reason field in the routingevent table(repository database) is populated with the value 'rona'			✓
Configuration for the Aux rona reason code.			✓
Automatic public chat disconnect when caller inactivity crosses the disconnect interval set in ICM			✓

* Product has been tested with the specified minor versions.

** There are limitations in using Advocate Admin and Workflow Designer. Refer to the Known Issues section.

*** IC 7.3.2 FP obsoletes PSN004146

Features not supported

- **Same Time Feature**

  The Same Time feature from Webagent is no longer supported from IC 7.3 release.

  Note: The Web agent's toolbar shows the Same Time button but the button does not work as the functionality is not supported.

- **Using Drop button on Hard phone**

  CM does not support using the Drop button on the hard phone for releasing a contact. Agents must use the Release button for releasing the contact. The purpose of the Drop button is to drop the last party added to the conference. Using the Drop button on the hard phone for releasing a call with only two parties involved might lead to unpredictable behavior in IC.

  IC Agents must use soft phone buttons to perform call operations.

Web browsers tested in IC 7.3.2 Feature Pack

Avaya IC includes support for several Web browsers for **End-Customer Chat Escalations** in IC 7.3.x Service Pack. The following list includes latest browser versions tested at the time of release of this FP:

Web browser
Chrome 33
Safari 7.0.2
Opera 20
Mozilla Firefox 28

Web browser
Microsoft Internet Explorer 8, 9 and 10

Important: Internet Voice (IV) Chat and Collaboration features are supported in Microsoft Internet Explorer only.

IC 7.3.x interoperability with OA 7.3.x

	OA 7.3	OA 7.3.1	OA 7.3.2
IC 7.3	✓	✓	
IC 7.3.1		✓	✓
IC 7.3.2			✓

Note: For information about the OA 7.3.2 release, see the Operational Analyst 7.3.2 Release Notes.

IC 7.3.x interoperability with Communication Manager and AES

This section describes the compatibility of IC 7.3.2 with Communication Manager and AES versions.

Communication Manager Compatibility matrix:

Communication Manager / Avaya Aura® Communication Manager	Telephony Server running on the operating system
5.x, 6.0, 6.2 and 6.3	Windows 2008 R2, Solaris 10 and AIX 6.1
Communication Manager / Avaya Aura® Communication Manager	Telephony Server running on the operating system
5.x, 6.0, 6.2 and 6.3	Windows 2008 R2, Solaris 10 and AIX 6.1

Avaya Application Enablement Services (AES) / Avaya Aura® AES compatibility matrix:

AES 6.1 with CVLAN client 6.1 on Windows 2008 R2 AES 6.1 with CVLAN client 3.1 on Solaris and AIX	Certified

AES 6.2 with CVLAN client 6.2 on Windows 2008 R2 AES 6.2 with CVLAN client 3.1 on Solaris and AIX	Certified
AES 6.3 with CVLAN client 6.3 on Windows 2008 R2 AES 6.3 with CVLAN client 3.1 on Solaris and AIX	Certified

Feature comparison of Avaya Agent Clients

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

Channel / Feature	Functionality Supported	Avaya Rich Client	Avaya Web Client	Avaya SDK Client	Avaya Siebel Native Client	Avaya Siebel Hybrid Client
Voice	Answer	✓	✓	✓	✓	✓
	Blind Transfer	✓	✓	✓	✓	✓
	Consult	✓	✓	✓	✓	✓
	Conference	✓	✓	✓	✓	✓
	Hold/Reconnect	✓	✓	✓	✓	✓
	Wrap	✓	✓	✓	✓	✓
	Transfer to Virtual Queue	✓	✓	✓	✓	×
	Switch to caller	✓	✓	✓	×	×
	Transfer to Agent	✓	✓	✓	✓	✓
Email	Reply / Reply All	✓	✓	✓	✓	✓
	Forward	✓	✓	✓	✓	✓
	Defer	✓	✓	✓	✓	✓
	Use local/global resource for responses	✓	✓	×	×	×
	Dismiss	✓	✓	✓	×	✓
	Transfer to Agent	✓	✓	✓	×	✓

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	✓	✓	✓	✓ *	×
	Wrapup Codes	✓	✓	✓	×	✓
	HTML Editor HyperLink toolbar button	✓	×	×	×	×
	Ability to download and use pre-configured email templates	✓	✓	×	×	×
Chat	Answer	✓	✓	✓	×	✓
	Transfer to Agent	✓	✓	✓	×	×
	Conference	✓	✓	✓	×	✓
	Wrap	✓	✓	✓	×	✓
	Co-browse	✓	✓	×	×	✓
	Emoticons	✓	✓	✓	×	✓
	Chat Typing status	✓	✓	✓	×	✓
	Join Us	✓	✓	✓	×	✓
	Transfer to Virtual Queue	✓	✓	✓	×	✓
Contact History	View	✓	✓	✓	×	×
	Filter	✓	✓	✓	×	×
Supervisor	Monitor/Un-Monitor	✓	✓	✓	×	✓

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

Channel / Feature	Functionality Supported	Avaya Rich Client	Avaya Web Client	Avaya SDK Client	Avaya Siebel Native Client	Avaya Siebel Hybrid Client
	Visible / Invisible	✓	✓	✓	×	✓
Multimedia Support		✓	✓	✓	×	✓
Selective After Call Work		×	×	×	✓	×

Product updates and patches

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

You can download the latest patches and installation instructions.

IC 7.3.2 Feature Pack installation and configuration guidelines

Perform the following steps to install IC 7.3.2:

Note: Skip the steps that are not applicable to your IC environment.

1. Ensure your system conforms to the prerequisites (Refer to Prerequisite guide of IC 7.3).
2. Ensure that you have a 7.3 License Key before proceeding.
3. Ensure that you have received all the installation files for the IC components included in the IC 7.3.2 FP.
4. Explore the installation options for installing the IC 7.3.2 FP.
5. Logout agents and stop all IC clients.
6. Stop IC servers, IC services, and Administration and Design.
7. Install IC Servers.
8. Install the Siebel Integration Component.
9. Install the Avaya Agent Web Client Connector.
10. Install the Avaya Agent Web Client.
11. Install Administration and Design.
12. Install Avaya Agent.
13. Start IC Servers, IC Services, and Administration and Design.
14. Perform the following configuration procedures:
    a. Configure all servers.

b. Configure SDK Server.
c. Configure Web Services.
d. Configure Design and Admin.
e. Configure Avaya Agent.
f. Configure Avaya Agent Web Client.
g. Configure the IC - Siebel integration.

15. Start Avaya Agent Web Client.

IC Scripts customization merges Carefully review the installation instructions as well as the list of files being installed from every package. The files, which have been changed as a part of the SP, replace the files that exist on the system in the respective folders. If the current installation at the customer site involves configuration changes or customization in any of the files that are being replaced by the SP Installer, backup the original file in a separate folder to identify old configuration or customization content. After the installation is successful, review the content of the new file that has been installed and merge the previous configuration or customization in the new file. Do not replace the new file with the old one directly as it might result in loss of new content.

- Enhancements in IC7.3.2 FP
- Enhancements in IC7.3.1 Service Pack

Enhancements in IC 7.3.2 Feature Pack

New Features and Enhancements

Please refer to What's New in Interaction Center Release 7.3.x guide available at

http://support.avaya.com/

Security Enhancements

This section provides list of security vulnerabilities that are addressed in IC 7.3.2 FP.

1. GRIP 11644: DWR object used on AIC HTML Client is subject to Vulnerability
2. GRIP 11641: Cross Site Scripting fixes on the AIC Admin Website module
3. GRIP 11655: HttpOnly cookie flag for HTML Client in IC
4. GRIP 11643: Cross Site Scripting fixes on the AIC Agent Web Client
5. wi01160342: Security scan found vulnerabilities in Admin and Public website
    a. Cross-Site Scripting
    b. Session Fixation
    c. Missing Cross-Frame Scripting Protection
    d. Parameter Based Redirection
    e. Server Error Response

6. wi01124008: Authentication Credentials Submitted In Plaintext for Admin Website
7. wi01124016: IC Website pages have inadequate URL Redirect Validation
8. wi01124020: IC Admin website pages doesn't have logout option
9. wi01123998: A malicious user is capable of injecting arbitrary JavaScript content into a user's browsing session of IC public website through Cross Site Scripting.
10. wi01124013: A malicious user is capable of injecting arbitrary JavaScript content into a user's browsing session on Admin Website through Cross Site Scripting.
11. wi01124021: A malicious user is capable of injecting arbitrary JavaScript content into a user's browsing session of AAWC through Cross Site Scripting.
12. wi01132046: HTTP Connector server exposes Generic Web Server Directory Traversal Vulnerability
13. wi01132047 : Man-in-the-middle attacker can force the communication to a less secure level as IC Directory server accepts sslv2 connections
14. wi01158433: RLManager allows operations like add/mod/del by extracting information from existing cookies

Please refer to Avaya Interaction Center Release 7.3.x Security Guide 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 working memory of a computer program at a specific time, when the program terminates abnormally or crashes. Core dumps assist in diagnosing and debugging errors in computer programs. Other key pieces of the program state including the processor registers, which may include the program counter and stack pointer, memory management information, and other processor and operating system flags and information, are also dumped at the same time.

Core dumps are useful debugging aids in several situations. Core dumps allow a user to save a crash for later or off-site analysis, or for comparison with other crashes. Core dumps can be used to capture data freed during dynamic memory allocation and may thus be used to retrieve information from a program that is no longer running. In the absence of an interactive debugger, a programmer can use the core dump to determine the error from direct examination.

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 interpret dumps, identifying variables symbolically and displaying source code. If the symbol table or file is not available, it is difficult to interpret the dump. There are also special-purpose tools called Dump Analyzers to analyze dumps.

If IC does not function according to the expected behavior, the reason might be incorrect implementation of business requirement or incorrect usage 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 usage of coding language and OS/Library APIs, it might be difficult to resolve the problem with the help of application logs only. Unavailability of the opportunities of live debugging on customer's production system 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. Core dump is created automatically in application crash scenarios. In other scenarios, where a process is still running, creating a core dump is similar to selecting the server in IC Manager, and then clicking a toolbar button.

Using the Simplified IC Dump feature, the IC Application can:

1. Create core dump with correct bitness, that is, 32-bit core dump.
2. Create full memory core dump file of the process.
3. Create core dump automatically on crash 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 platforms such as Windows, Solaris and AIX, is done automatically by the Service Pack installer.

IC WebServices service configuration for Windows platform

Perform the following steps on the machine where the IC WebServices service is configured for the Windows platform:

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.

Detailed steps to start, stop, remove or deploy WebServices service are available in the Deploying Web Services chapter of the Installation and Configuration guide.

Note:

Alternatively, you can 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.

Enabling fullcore on AIX

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

Core dump creation when IC process crashes

A core dump generated in a crash scenario, with the right set of information contained within it, is useful in finding the root cause of the coding issue through the postmortem debugging. The Simplified IC Dump feature enables all IC processes such as a Toolkit server and client to create the full memory core dump file automatically at the IC install location.

The Simplified IC Dump feature names the core dump file using the component name and the time when the crash occurred.

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

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 core dump file with name *ADU_Voice1(adusrv.exe)[1234]_Crash-20130301112345.dmp* is created in *<AVAYA_IC73_HOME>\logs* folder.

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

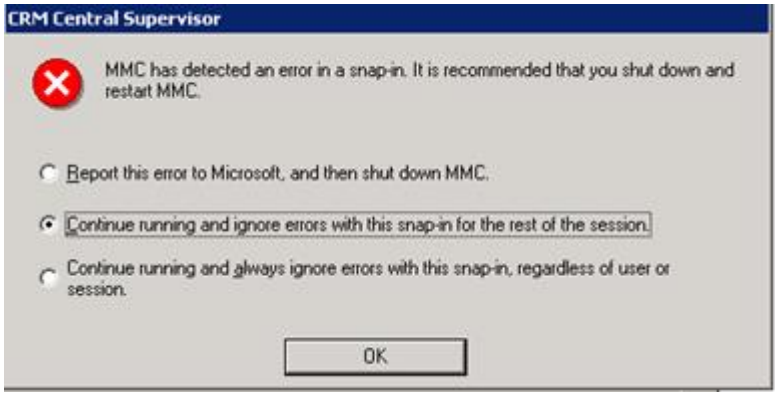
application with process id 2345 crashes at 10:39:56 AM on 01 March 2013 when Agent with login id agent1 was logged in, then the core dump file with name *agent1(qui.exe)[2345]_Crash-20130301103956.dmp* is created in <*AVAYA_IC73_HOME*>*logs* folder.

Note:

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

2. The core dump file is created by the IC implemented unhandled exception filter hook code. The core dump is created 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 crash scenarios, Windows Error Reporting or other similar methods and utilities can be used 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 in case of crash within MMC.



Select the '*Continue running and ignore errors with this snap-in for the rest of the session*' option in the dialog box.

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 core dump file with the name adusrv.exe[1234]_Crash-1362137025.core is created in <AVAYA_IC73_HOME>/logs folder. 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 core dump file with the name java[2345]_Crash-1362134396.core is created in <AVAYA_IC73_HOME>/logs folder.

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 core dump file will be created by Solaris OS.

Crash dump on AIX platform

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

The name of the core dump file is *core.PID.<TimeStamp>* if there is no JVM loaded in the process memory irrespective of whether JVM is loaded explicitly or implicitly. In such a case, the core dump file is created by AIX OS. 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 core dump file with name *core.1234.01112345* is created in the *<AVAYA_IC73_HOME>/etc* folder.

Note:

The TimeStamp is in the format of DDHHMMSS in the previous example.

The name of the core dump file is *core.<TimeStamp>.PID.<SequenceNo>.dmp* if there is JVM 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 core dump file with name *core.20130301.103956.2345.0001.dmp* is created in *<AVAYA_IC73_HOME>/bin* folder.

Note:

If the core dump creation is controlled by JVM, the TimeStamp 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

It is easier to troubleshoot some problems through core dump of the process even though the process does not crash and is in a running state. You can rectify scenarios like application hang, thread deadlock, memory or handle leak through postmortem debugging of core dump of the running application along with analyzing the application log.

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

The core dump file of a running server is created in the <AVAYA_IC73_HOME>/logs directory on all three platforms. Following are the names of core dump files on different platforms created through IC Manager:

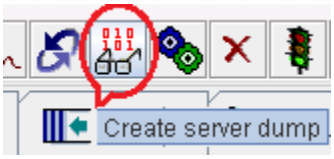
1. **Windows:** *<ServerAlias> [PID]_Dump-<TimeStamp>.dmp*
2. **Solaris:** *<ServerAlias> [PID]_Dump-<TimeStamp>.core.PID*
3. **AIX:** *<ServerAlias> [PID]_Dump-<TimeStamp>.core*

Note: The TimeStamp is calculated using *localtime_s* API on Windows and localtime 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 for creating the core dump.

   Note: You can select multiple servers in IC Manager for creating core dump.
3. Select the '*Create server dump*' button on the Toolbar as shown in the following image:



Alternatively, you can also use, the '*Dump*' popup menu by right-clicking the selected servers.

Another method of creating a dump is to select *Server* → *Dump*.

4. Select '*Yes*' on the confirmation dialog box.

The info alarm is displayed confirming successful creation of core dump of the selected servers. In case 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:

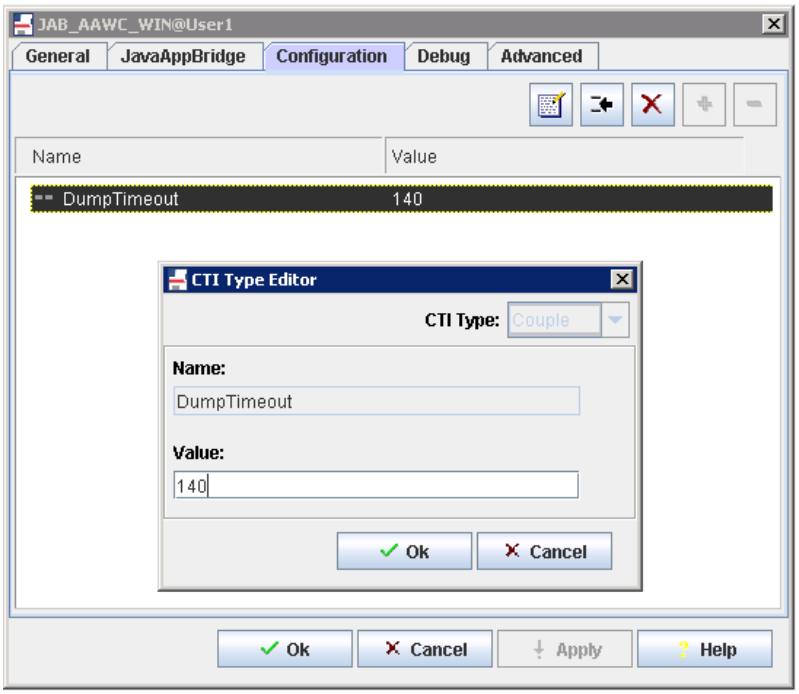
1. IC Manager first pings the selected server by sending a Ping VESP request.
2. If the response to ping is successful, then IC Manager calls the selected server's Dump VESP method.
3. If Server.Ping or Server.Dump VESP request fails, then IC Manager sends request to corresponding ORB server to create the selected servers core dump.
4. If the ORB is the parent process of the selected servers, then ORB creates core dump for that server. This is a backup mechanism for creating core dump.
5. IC Manager raises an alarm notifying the success or failure of the core dump creation.

Note:

1. By launching a separate utility as a separate process and providing a process ID of the selected server as an argument to that utility process, you can create dump of a running server. The Simplified IC Dump feature uses *<AVAYA_IC73_HOME>\bin\avayadmp.exe*, *gcore* and *gencore* utilities for core dump creation on Windows, Solaris and AIX platforms respectively. *Avayadmp.exe* utility is a part of the IC 7.3.1 Service Pack. On Solaris and AIX, *Avayadmp.exe* is required to ensure that respective utilities, that is, *gcore* and *gencore* are installed and their 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 should not be created unnecessarily as it may 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. In case of automatic Core dump creation due to an application crash, the issue, along with core dump and application log file, must be reported to Avaya support. To speed up the resolution of the issue, provide the crash scenario and steps along 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. The minimum value of this parameter is 20 seconds, the maximum value is 160 seconds, and default value is 64 seconds. You can add the *DumpTimeout* parameter to the configuration tab of any server in IC Manager in the form of a new seqCouple.



After adding or changing the *DumpTimeout* parameter in IC Manager, select Server -> Update to activate the added parameter or updated value.

Note: This configuration parameter does not play any role in creating core dump due to application crash. In most of the cases, you would not be required 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 dump of a running process cannot be created through IC Manager on the Windows platform, then the new avayadmp.exe application present in <AVAYA_IC73_HOME>\bin folder can be directly used for dump creation through the command prompt. Avayadmp.exe can be 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]

-p

- Mandatory Parameter. Process ID of the application to be dumped.

-t

- Optional Parameter. Type of dump. Values could be (tiny, mini, midi or full).
- If not provided, then full dump will be created.

-l

- Optional Parameter. A valid dump location or directory where dump will be saved.
- If the location or directory is not provided, then dump will be saved in Windows Temp folder.

-n

- Optional Parameter. Friendly application name. For example, alias name.
- If not provided, then exe name will be used to name the dump file.

-d

- Optional Parameter. Valid directory of dbghelp.dll library.
- If not provided, then dbghelp.dll be tried first from application's directory and then from Windows System directory.

Example: If the Avaya Agent Web Client process is not able to process any VESP request, then it would not be possible to create the dump of AAWC through IC Manager's '*Create server dump*' toolbar button. In such scenarios, the ORB server also does not help in creating the dump since the AAWC process is launched separately and it 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 directory.

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 check if the core dump file is created at the specified location with the name as <ServerAlias>[PID]_Dump-<TimeStamp>.dmp.

Note: In case of other supported platforms, that is, Solaris and AIX, the respective dump creation utilities such as gcore and gencore can also be used in a similar manner from the command line to create the dump.

Examples:

Solaris: *gcore -o <AVAYA_IC73_HOME>/logs/<core dump file name> ProcessID*
AIX: *gencore ProcessID <AVAYA_IC73_HOME>/logs/<core dump file name>*

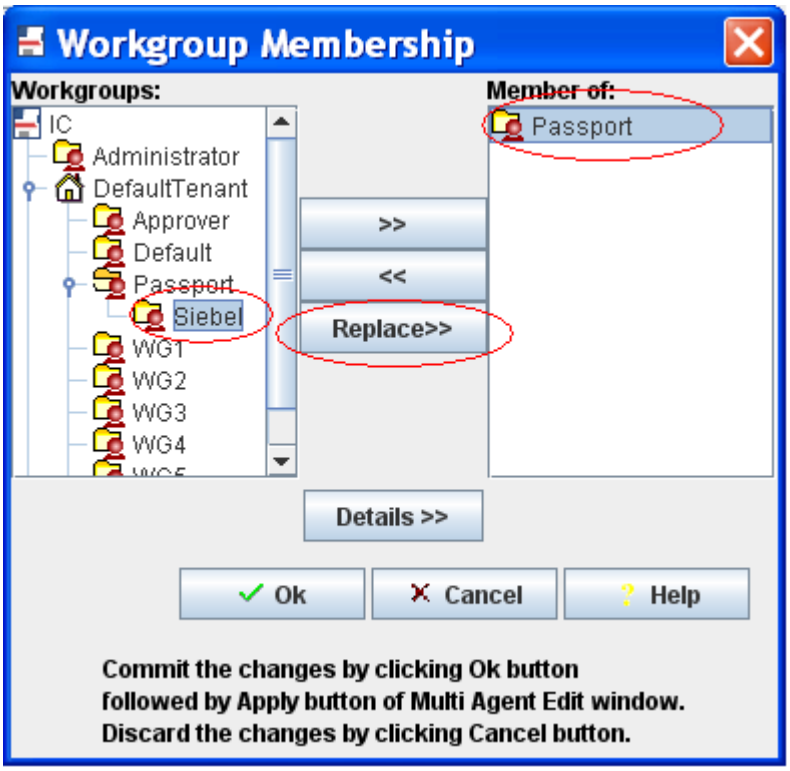
For more information on how to use gcore and gencore, refer to the respective platform manual.

Replace Workgroup Functionality

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

In the Workgroup Membership window, a new button Replace>> has been added along with the add member (>>) and remove member (<<) buttons.

To perform the Replace operation, the user has to select an existing workgroup membership from the *Member of* list on the right side and a replacement from *Workgroups* on the left side and click the Replace>> button as follows:



The scenarios with steps to perform the Replace operation are as follows:

Scenario 1:

All the selected agents belong to only one workgroup and all agents must move to another workgroup.
For example, move all agents from *Passport* workgroup to S*iebel* 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 the three buttons Add (>>), Remove (<<) and *Replace*>> are activated.
4. Click the *Replace*>> button 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.

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

Before performing *Replace:*

Agent	Workgroup name	Value of the *workgrouporder* field in the groupmember table

agent1	Passport	0
agent2	Passport	0
agent3	Passport	0

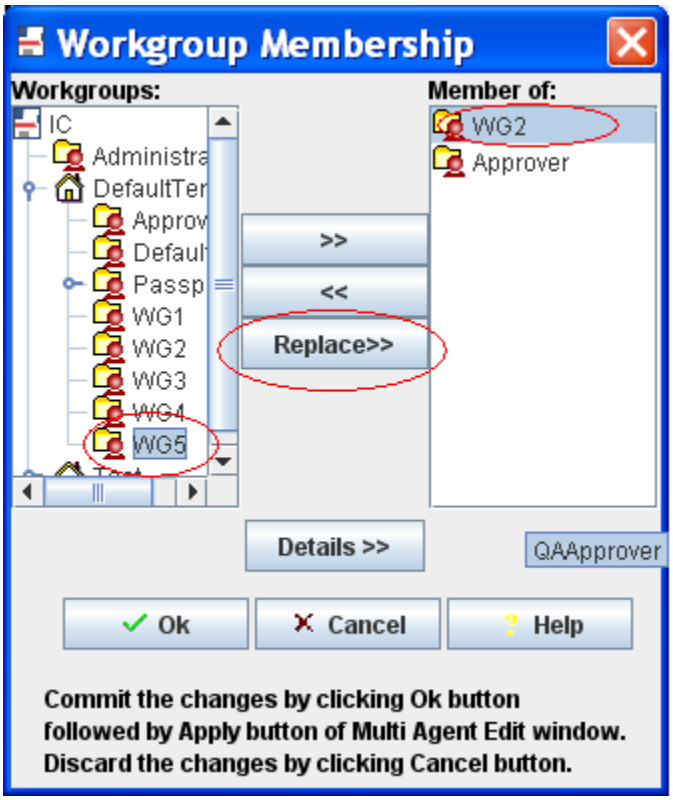
After performing *Replace:*

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

Scenario 2:

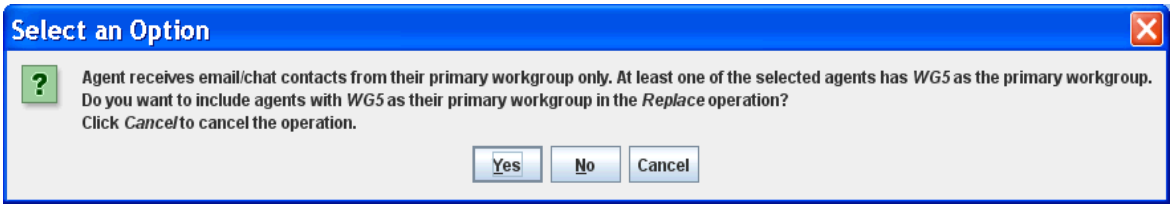
The selected agents belong to multiple workgroups. You must replace one of the common workgroups that agents belong to with a new workgroup.

For example, remove WG2 and replace WG2 with WG5 as shown in the following image:



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 the three buttons Add (>>), Remove (<<) and *Replace*>> are activated.
4. Click the *Replace*>> button to move the agents from the original workgroup to the new workgroup.
5. If some of the selected agents have the new workgroup as their primary workgroup, that is, *workgrouporder* for the workgroup is zero, the following message appears:



a. On selecting *yes*, the original workgroup is replaced by the new workgroup for all the agents.

The database changes after selecting the *Yes* option are as follows:
Before performing *Replace*:

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

After performing *Replace*:

Agent	***Workgroup name***	***Value of the workgrouporder field in the groupmember table***

agent1	Default **WG5** Approver	**0** 1 2
agent2	**WG5** Approver	**0** 1
agent3	**Approver**	**0**
	WG5	**1**

b. On selecting *No*, the agents who have the original workgroup as their primary workgroup are skipped and the replace operation is performed for other selected agents.
The database changes after selecting the *No* option are as follows:

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

c. On selecting Cancel, the Replace operation is canceled.

Other changes in the Agent Multi-Edit operation:

1. **Only one operation at a time:**
   Only one operation out of add, remove or replace is allowed 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 has been updated 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 the agents being edited; only the common workgroups across all the agents are displayed in the *member of* field.
3. **Adding new workgroup:**
   If a new workgroup is added in the *member of* list, the workgroup is added at the last position in the *member of* list for each individual agent.
4. **Removing workgroup from common member's list:**
   If any workgroup is removed from the *member of* list, the workgroup is removed from all the agents being edited. The order of the workgroups that is present after the workgroup being removed is pushed up by 1.
5. **Workgroup re-ordering:**
   Member re-ordering, 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.

Internet Explorer 10 support for chat escalation

Customers can use Internet Explorer 10 for chat and collaboration from SP 7.3.1 onwards. Use of IE 10 on the Agent side is not supported.

The following functionality is supported for end customers using IE 10:

1. Escalate a chat contact
2. Co-browse
3. Collaborative Form filling

Note: IE 10 in IE 9 Mode, IE 10 in IE 8 mode and IE 10 in Quirk mode are not supported.

Installation

This section describes the FP Installer that updates the existing Avaya IC 7.3 systems with the Avaya IC 7.3.2 FP 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 is replaced by the installer with new files.
2. Copies the new IC 7.3.2 files into the appropriate directories 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/7.3.2/<FolderNameOfComponent>/Log/install.log
```

Where **<FolderNameOfComponent>** is the folder name of each component where the respective component files reside.

The Installation Tool provides a separate installation program for each IC component. The Installation Tool helps you to upgrade your machines based on the component they run. The following table lists the name of the component and its respective folder name:

Component/machine	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:

- Un-registers the necessary files on your system.
- Registers the new files on your system.

Before you install

You must have separate machines for each IC component. Avaya does not support multiple IC components installed on the same machine. 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 an IC installation is being done on a fresh system using the RTM installer, then some error messages can popup during the installation of the FP. These error messages state that the file being copied during the FP 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 FP installer.

When installing IC using the RTM installer, the installer adds data regarding the installation location of IC to some of the files being installed by the installer. 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 FP, then it may happen that some of the files in the FP 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 FP installation. You can ignore the error message and continue with the installation by choosing the Replace option on the dialog box that pops up.

Stop Avaya Agent Web Client

Before you run the IC 7.3.2 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

1. For Windows Operating System, click **Start** > **Run** to open the command prompt.
2. Change the directory to: AVAYA_IC73_HOME\IC73\bin.
3. Execute the following command:

Operating System	Procedure
Windows	To stop: **aawcclient.bat stop**

Operating System	Procedure
Solaris and AIX	To stop: `./aawcclient.sh stop`

Stop IC services

Before you run the IC 7.3.2 Server installation, you must stop all the IC services and ensure those services are stopped. This might take several minutes because it allows the servers to complete their current tasks before shutting down.

Windows

To stop the IC Services:

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 Voice Media Manager
- Avaya SDK Services
- Avaya Business Advocate Component Manager

Solaris and AIX

To stop the IC Services:

1. Log in with root privileges and navigate to the **`../IC73/bin`** directory:
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

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.**

- For IBM http Web Server
    1. Change the directory to: AVAYA_IC73_HOME\IC73\bin
    2. At the command line, type: **`./httpserver.sh stop`**
    3. Press **Enter**.

Stop the VMM service (Solaris only)

If you host your Avaya IC servers on Solaris and have the VMM service configured, you must stop the VMM setup service to configure the Voice Media Manager (VMM) for Voice Chat. The VMM setup service configures the VMM to start automatically.

You must only perform this step if you host your Avaya IC servers on Solaris. Do not perform this step if you host your servers on Windows machines.

To stop VMM on Solaris:

1. Navigate to the following directory: IC_INSTALL_DIR/IC73/bin
2. Type the following at the command line:

   `./vmm_setup stop`
3. Press **Enter**

Stop IC servers

Before you run the IC 7.3.2 Server installation, you must stop all the IC servers and ensure all processes are stopped. Ensure that all IC Avaya Agents and IC Avaya Agent Web Clients are logged off prior to stopping all IC servers. This may take several minutes because the servers need to 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 the IC servers in the proper order using IC Manager:

1. Start IC Manager, if it is not already running.
2. Click the **Server** tab.

3. Select **Server** > **Shutdown**.
4. Select the IP address or the name of the machine 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 machine:

1. In a command window, navigate to the **`...\IC73\bin`** directory.
2. Stop all IC servers:

- To stop IC servers on all/multiple machines (multi-box setup):
  i. At the command prompt, enter the command: **`icadmin tva <username> <password>`**.
  ii. Press **Enter**.
- To stop IC servers on one system:
  i. At the command prompt, enter the command: **`icadmin tv <username> <password>`**.
  ii. 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 machine:

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 and AIX

IC Manager

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

1. Start IC Manager, if it is not already running.
2. Click the **Server** tab.
3. Click **Server** > **Shutdown**.
4. Select the IP address or the name of the machine 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 machine:

1. In a command window, navigate to the **`.../IC73/bin`** directory.
2. Stop all IC servers:

- To stop IC servers on all/multiple machines (multi-box setup):
  i. On the command line, enter the command: **`./icadmin tva <username> <password>`**.
  ii. Press **Enter**.
- To stop IC servers on one machine:
  i. On the command line, enter the command: **`./icadmin tv <username> <password>`**.
  ii. 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 machine.
3. Check to ensure the IC servers are not running.

Solaris and AIX

1. At the command line, 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. Check to ensure the IC servers are not running.

If any processes related to IC servers are still running, terminate all the processes related to IC servers.

4. To terminate multiple processes with one command, type the following command:

`kill -9 <PID>`

Where PID is the Process ID of each individual process that is related to IC servers.

Note: Alternatively, you can type "**`kill -9 <PID1> <PID2>.... <PIDn>`**" to end all the processes with a single command.

5. Press **Enter**.

Prerequisites

This section describes the prerequisites for installing the IC 7.3.2 Service Pack.

Prerequisites for installing IC 7.3.2

1. Before you install IC 7.3.2, you must have IC 7.3 installed on your system.
2. Cumulative Security Update for Internet Explorer 8 (KB978207) must be installed on the machines from where AAWC is launched.

Note: Microsoft might have released patch superseding this and the same can be installed.

Getting Started

Avaya IC 7.3.2 is available on the Avaya Support Web site at: http://support.avaya.com/downloads/

To receive the IC 7.3.2 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 is supplied to assist you in requesting your license keys.

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

Creating License Request

Perform the following steps to create the license request:

1. License Key Request (New)

   Send to: icoakeyrequest@avaya.com

   Provide the following details:

   - Customer Name
   - Customer Location (city, state, country)
   - Avaya SAP Order Number
   - MAC Address (HostID for Solaris) of all Servers running WebLM Service
   - System Purpose (for example, Production, Test, Lab)

- Return Email address
- Implementer of system (Avaya PSO, Avaya Business Partner or SI, self)

2. License Key Request (Addition/change)

Send to: icoakeyrequest@avaya.com

Provide the following details:

- COPY OF CURRENT LICENSE FILE (IMPORTANT)
- Customer Name
- Customer Location (city, state, country)
- If adding - Avaya SAP Order Number
- Avaya Customer Number
- If changing - MAC Address (HostID for Solaris) of all Servers running WebLM Service
- System Purpose (for example, Production, Test, Lab)
- Return Email address
- Implementer of system (Avaya PSO, Avaya Business Partner or SI, self)

Downloading the IC 7.3.2 Feature Pack

You can download the IC 7.3.2 Service Pack files from the Avaya Support site: http://support.avaya.com/downloads/.

To download IC 7.3.2:

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 the **Downloads** option.
5. Click **Enter**.
6. Click the appropriate IC 7.3.2 file name to download the respective file.
7. Move the IC 7.3.2 files to an installation directory on the system where you want to store them.

Important: The name of the installation directory 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 directory that contains any other special characters in its name.

Installation files

The following table indicates the machine type, operating system, and the filename for each of the IC 7.3.2 components:

Note: The mapped network drive installation option is not available for the Solaris and AIX platforms.

Component/machine	Platform	Filename

Component/machine	Platform	Filename
Administration and Design	Windows	IC732WinAdmin.zip. Extract the files into the install directory on the local machine or on the mapped network drive, depending on the installation option you want to follow.
Avaya Agent client	Windows	IC732WinAgentClient.zip. Extract the files into the install directory on the local machine or on the mapped network drive, depending on the installation option you want to follow.
Avaya Agent Web Client	Windows	IC732WinWebClient.zip. Extract the files into the install directory on the local machine or on the mapped network drive, depending on the installation option you want to follow.
Avaya Agent Web Client Connector	Windows	IC732WinWebConnector.zip. Extract the files into the install directory on the local machine or on the mapped network drive, depending on the installation option you want to follow.
	Solaris	IC732SolWebConnector.tar. Extract the files into the install directory on the local machine.
	AIX	IC732AixWebConnector.tar. Extract the files into the install directory on the local machine.
IC Servers	Windows	IC732WinServer.zip. Extract the files into the install directory on the local machine or on the mapped network drive, depending on the installation option you want to follow.
	Solaris	IC732SolServer.tar. Extract the files into the install directory on the local machine.
	AIX	IC732AixServer.tar. Extract the files into the install directory on the local machine.
Siebel Integration component (IC side)	Windows	ICSide732win.zip. Extract the files into the install directory on the local machine or on the mapped network drive, depending on the installation option you want to follow.
	Solaris	ICSide732sol.tar. Extract the files into the install directory on the local machine.
	AIX	ICSide732aix.tar. Extract the files into the install directory on the local machine.

Component/machine	Platform	Filename
Siebel Integration component (Siebel side)	Windows	SiebelSide732win.zip. Extract the files into the install directory on the local machine or on the mapped network drive, depending on the installation option you want to follow.
	Solaris	SiebelSide732sol.tar Extract the files into the install directory on the local machine.
	AIX	SiebelSide732aix.tar Extract the files into the install directory on the local machine.

Installation options

Avaya IC 7.3.2 provides the following installation options:

Network installation with mapped drive

Local installation

Silent installation

Console installation

The IC Server components, Siebel Integration component [Siebel side], Siebel Integration component [IC side], and Avaya Agent Web Client Connector components are installed on the Windows, Solaris, and AIX platforms. All other components are installed on the Windows platform only.

For information on all the supported platforms for IC, see IC 7.3 Installation Planning and Prerequisites.

Network installation with mapped drive

You can install IC 7.3.2 from a network (shared) computer to upgrade other machines without having to copy the IC 7.3.2 files from the central computer to those machines.

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

Note: If Universal Naming Convention (UNC) is not supported, you must map the drive to be accessed from the installation machine. 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 machines, copy the component directory, for example, Server, Avaya Agent, or Avaya Web Agent Client from the central machine to the machine where you want to install the component.

Silent installation

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

1. Go to the package directory where the contents of the FP installer are extracted.
2. At the command prompt, type:

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

   For example,

Operating System	Command
Windows	setupwin32.exe -options-record "D:\temp\SP732Silent.opt"
Solaris	./setupsolarisSparc.bin -options-record "/tmp/SP732Silent.opt"
AIX	./setupaix.bin -options-record "/tmp/SP732Silent.opt"

   Note: The <setupfile> is the platform-specific name of the setup executable and <AbsolutePathOfFile.ext> is the qualified file name, where "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 machine where you want to install.
2. Go to the package directory where the contents of the Feature Pack installer are extracted.

   At the command line, type:

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

   For example,

Operating System	Command
Windows	**setupwin32.exe -options "D:\temp\SP732Silent.opt" -silent**
Solaris	**./setupsolarisSparc.bin -options "/tmp/SP732Silent.opt" -silent**
AIX	**./setupaix.bin -options "/tmp/SP732Silent.opt" -silent**

The <setupfile> is the platform-specific name of the setup executable and <AbsolutePathOfFile.ext> is the qualified file name, where "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:

1. 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`

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

Order of installation

After you complete the instructions for a network installation or a local installation, install the IC 7.3.2 components in the following order:

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 7.3.2 Server component. The Server component can be installed on the Windows, Solaris, and AIX platforms.

This section includes the following topics:

Windows installation procedures

Solaris installation procedures

AIX installation procedures

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

Windows installation procedures

Note: The server installation instructions in this section pertain to existing IC setup on the Windows 2003 server. For installation of IC on the Windows 2008 R2 server, refer to the relevant chapter in this document.

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

1. Before you begin the FP Installation, ensure that all IC components are stopped as explained in the sections, Stop IC servers and Stop IC services.
2. Go to the directory where you extracted the contents of the IC732WinServer.zip file.
3. Copy the IC732WinServer folder to the machine 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.
4. Open the IC732WinServer folder and double-click setupwin32.exe to start the installation program.
5. At the Welcome screen, click **Next** to continue.
6. At the next screen that displays the location of the Uninstall program, click **Next**.
7. In the pop-up window that prompts Please stop all Avaya IC servers and services, click **Continue**.
8. On the next screen, which displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

1. Creates a backup directory and moves the existing server files to that directory.
2. Copies the new server files to the proper directories.
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\7.3.2\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

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, take the backup of the tssrv.exe and tssrv.pdb files, and delete the files from their current location. Make a copy of the files for your switch and rename the copies to tssrv.exe and tssrv.pdb.

For example: For Avaya DEFINITY/CM, create a copy of cvlansrv.exe and rename it as tssrv.exe in the AVAYA_IC73_HOME\bin directory. Similarly, create a copy of cvlansrv.pdb and rename it as tssrv.pdb in the AVAYA_IC73_HOME\bin directory.

Switch	Copy...	Rename to...
Avaya DEFINITY/CM	cvlansrv.exe, cvlansrv.pdb	tssrv.exe, tssrv.pdb
Nortel Meridian	ctsrv.exe, ctsrv.pdb	tssrv.exe, tssrv.pdb
Aspect Call Center	tsv5aspectcmi.exe, tsv5aspectcmi.pdb	tssrv.exe, tssrv.pdb
Cisco ICM	tsv5cisco.exe, tsv5cisco.pdb	tssrv.exe, tssrv.pdb

9. If a TSQS Server is configured, take a backup of the tsqssrv.exe and tsqssrv.pdb files, and delete the files from their current location. Make a copy of the files for your switch and rename the copies to tsqssrv.exe and tsqssrv.pdb.

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

Switch	Copy...	Rename to...
Avaya DEFINITY/CM	tsqssrv_asai.exe, tsqssrv_asai.pdb	tsqssrv.exe, tsqssrv.pdb
Nortel Meridian	tsqssrv_rti.exe, tsqssrv_rti.pdb	tsqssrv.exe, tsqssrv.pdb
Aspect Call Center	tsqssrv_ aspctportal.exe (no .pdb file)	tsqssrv.exe
Cisco ICM	tsqssrv_cisco.exe, tsqssrv_cisco.pdb	tsqssrv.exe, tsqssrv.pdb

10. On the Web Management Services IC machine, delete the folder "localhost" from the following location:

`../IC73/tomcat/work/Catalina/.`

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

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

Note: In September 2012, Avaya has announced End of Sale (EoS) for Avaya IC's support for third-party switches (PABXes) vide End of Sale Notice: https://downloads.avaya.com/css/P8/documents/100166179. As noted in the EoS notice, the End of Manufacturing Support for third-party switches will be effective December 2013. Refer to the End of Sale Notice for more details.

Solaris installation procedures

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

1. Before you begin the FP Installation, ensure that all IC components are stopped as explained in the sections, Stop IC servers and Stop IC services.
2. Go to the directory where you uncompressed the contents of the IC732SolServer.tar file.

3. At the command line, type: $AVAYA_IC73_HOME/bin/icenv ./setupsolarisSparc.bin (where $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. On the next screen, which displays the location of the Uninstall program, click **Next**.
6. In the pop-up window that prompts Please stop all Avaya IC servers and services, click **OK**.
7. On the next screen, this 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: Installation was successful. No errors or warnings were generated. Complete log messages are available at: .../IC73/ICServicePacks/7.3.2/Server/Log/install.log	If installation is unsuccessful, the system displays: ALERT! Installation failed. Please fix these errors and rerun the installer. The following errors or warnings were generated. Complete log messages are available at: .../IC73/ICServicePacks/7.3.2/Server/Log/install.log LIST OF ERRORS AND WARNINGS

8. Click **Finish**.
9. If the installation is unsuccessful, run the Uninstall program. Correct the errors and re-run the Installation program.
10. 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`**.

11. If the tssrv is a symbolic link to the Telephony Server, the system displays: lrwxrwxrwx filenameA -> filenameB (where filenameA is a variable for tssrv and filenameB is the absolute server name).
12. 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
Nortel Meridian	Ctsrv

13. 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 directory.

Switch	Copy	Rename to

Switch	Copy	Rename to
Avaya DEFINITY/CM	cvlansrv	tssrv
Nortel Meridian	ctsrv	tssrv

14. 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 directory.

Switch	Copy	Rename to
Avaya DEFINITY/CM	tsqssrv_asai	tsqssrv

15. 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 machine, delete the folder "localhost" from the location ".../IC73/tomcat/work/Catalina/". Execute this step on only the Web Management Services IC system.

AIX installation procedures

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

AIX installation prerequisites

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

1. Ensure that all IC components are stopped as explained in the sections, Stop IC servers and Stop IC services.
2. Change the directory to $AVAYA_IC73_HOME/lib.
3. At the command prompt, type: **`slibclean`**
4. 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`

5. 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.

6. 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.

1. Before you begin the FP Installation, ensure that all IC components are stopped as explained in the sections, Stop IC servers and Stop IC services.
2. Go to the directory where you uncompressed the contents of the IC732AixServer.tar file.
3. At the command prompt, type:

`export AVAYA_IC73_HOME=<Avaya IC Servers installation path>`

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

4. Press **Enter**.
5. At the command prompt, type: **`$ ./setupaix.bin`**.
6. On the Welcome screen, click **Next**.
7. On the next screen, which 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. 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

10. Click **Finish**.
11. If the installation is unsuccessful, run the Uninstall program. Correct the errors and re-run the Installation program.
12. 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.
13. If the tssrv is a symbolic link to the Telephony Server, the system displays: lrwxrwxrwx filenameA > filenameB (where filenameA is a variable for tssrv and filenameB is the absolute server name).
14. If the tssrv file is a symbolic link to the TS, use the existing file without renaming it.

Switch	Use

Avaya DEFINITY/CM	cvlansrv

15. 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. Create 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` directory.

Switch	Copy	Rename to
Avaya DEFINITY/CM	cvlansrv	tssrv

16. 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` directory.

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

17. On the Web Management Services IC machine, delete the folder "localhost" from the following location:

`.../IC73/tomcat/work/Catalina/.`

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

Siebel Integration Component installation

This section describes the installation procedures for the Siebel Integration Component of the Avaya IC 7.3.2 release. The Siebel Integration component is installed on the Windows, Solaris, and AIX machines 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

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

Siebel Integration component on Siebel server

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

1. Go to the directory where you extracted the contents of the SiebelSide732win.zip file.
2. Open the SiebelSide732win folder and double-click on setupwin32.exe to start the installation program.
3. At the Welcome screen, click **Next** to continue.
4. At the next screen, enter the path location for the Siebel Servers installation, click **Next**.

For example, `C:\seaxx\siebsrvr`.

5. On the next screen, which displays the location of the Uninstall program, click **Next**.
6. On the next screen that prompts, Please stop all Siebel Services before applying the patch, ensure that the Siebel Service is not running, and click **OK**.
7. On the next screen, this 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: `C:\Seaxxx\siebsrv\ICServicePack\7.3.2\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\7.3.2\SiebelSide\Log\install.log LIST OF ERRORS AND WARNINGS

8. Click **Finish**.
9. 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 machines that are running IC servers:

1. Go to the directory where you extracted the contents of the ICSide732win.zip file.
2. Open the ICSide732win folder and double-click on setupwin32.exe to start the installation program.
3. At the Welcome screen, click **Next**.
4. At the next screen that displays the location of the Uninstall program, click **Next**.
5. At the next screen that prompts, Please stop all IC Services before applying the patch, ensure that all IC Services are stopped, and click **OK**.
6. On the next screen, which 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: 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

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

Solaris installation procedures

The Siebel Integration component must be installed on the machine running Siebel Services and the machine 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 machines that are running Siebel Services.

1. At the command line, navigate to the directory where you uncompressed the contents of the SiebelSide732sol.tar file. If the file is compressed, untar the file using the tar -xvpf command.
2. At the command line, type the following command:

```
./setupsolarisSparc.bin
```

3. Press **Enter**.
4. On the Welcome screen, click **Next**.
5. At the next screen, enter the path location for the Siebel Servers installation, click **Next**. For example, root/seaxx/siebsrvr)
6. The next screen displays the location of the Uninstall program, click **Next**.
7. On the next screen, which prompts Please stop all Siebel Services before applying the patch, confirm the Siebel Service is not running and click **OK**.
8. On the next screen that displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

- 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/7.3.2/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/7.3.2/SiebelSide/Log/install.log LIST OF ERRORS AND WARNINGS

9. Click **Finish**.
10. If the installation was 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.

1. At the command line, navigate to the directory where you uncompressed the contents of the ICSide732sol.tar file.
2. At the command line, type the following command: **`./setupsolarisSparc.bin`**.
3. Press **Enter**.
4. On the Welcome screen, click **Next**.
5. On the next screen, enter the path location for the IC Servers installation and click **Next**.

For example, root/IC73

6. On the next screen displays the location of the Uninstall program, click **Next**.
7. On the next screen that prompts, Please stop all IC Services before applying the patch, ensure that the IC Services are not running, and click **OK**.
8. On the next screen that displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

- 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

9. Click **Finish**.
10. If the installation was unsuccessful, run the Uninstall program. Correct the errors and re-run the Installation program.

AIX installation procedures

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.

1. At the command line, navigate to the directory where you uncompressed the contents of the SiebelSide732aix.tar file.
2. At the command prompt, type: **`./setupaix.bin`**
3. Press **Enter**.
4. On the Welcome screen, click **Next**.
5. On the next screen, enter the location for the Siebel Servers installation, click Next.

For example, root/seaxx/siebsrvr

6. The next screen displays the location of the Uninstall program, click **Next**.
7. 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**.
8. 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: Installation was successful. No errors or warnings were generated. Complete log messages are available at: root/Seaxxx/siebsrv/ICServicePack/7.3.2/SiebelSide/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: root/Seaxxx/siebsrv/ICServicePack/7.3.2/SiebelSide/Log/install.log LIST OF ERRORS AND WARNINGS

9. Click **Finish**.
10. 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.

1. 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.
2. At the command line, type: **`./setupaix.bin`**.
3. Press **Enter**.
4. At the Welcome screen, click **Next**.
5. At the next screen, enter the path location for the IC Services installation, and click **Next**.

For example, root/IC73.

6. The next screen displays the location of the Uninstall program, click **Next**.
7. 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**.
8. 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

9. Click **Finish**.
10. If the installation was unsuccessful, run the Uninstall program. Correct the errors and re-run the Installation program.

Import the AICD.def file

To import the AICD.def file:

1. Start the Siebel Services.
2. Log in to the Siebel Thin Client call center application from the web browser as Siebel Administrator.
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 under the Configurations tab.

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.

6. Click **Next**.
7. Select the **Commands** check box.
8. Browse to the AICD.def file.
9. 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 7.3.2 release. Install the Avaya Agent Web Client Connector on the machine that hosts the Tomcat Server.

- Installation path procedures
- Windows installation procedures
- Solaris installation procedures
- AIX installation procedures

Installation path procedures

The IC 7.3.2 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:

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 and AIX

To declare the Avaya Agent Web Client Connector installation environment variable on Solaris or AIX:

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 described in the following section.

Windows installation procedures

Perform the following steps on the Windows machines that are running the Avaya Agent Web Client.

1. Before you begin the Service Pack Installation, ensure that all IC components are stopped as explained in Stop Avaya Agent Web Client.
2. Go to the directory where you extracted the contents of the IC732WinWebConnector.zip file.

3. Open the IC732WinWebConnector folder and double-click on setupwin32.exe to start the installation program.
4. On the Welcome screen, click **Next** to continue.
5. On the next screen, which displays the location of the Uninstall program, click **Next**.
6. On the next screen, which displays the installation summary, click **Next** to run the installation. The Installation Tool performs the following:

- Creates a backup directory and moves the existing web client connector files to that directory.
- Copies the web client connector files to the proper directories.
- Copies the files from the Java folder 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\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\7.3.2\WebConnector\Log\install.log LIST OF ERRORS AND WARNINGS

7. Click **Finish**.
8. If the installation is unsuccessful, run the Uninstall program. Correct the errors and re-run 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 machines that are running the Avaya Agent Web Client.

1. Before you begin the Service Pack Installation, ensure that all IC components are stopped as explained in Stop Avaya Agent Web Client.
2. Go to the directory where you uncompressed the contents of the IC732SolWebConnector.tar file.
3. At the command prompt, type: **`./setupsolarisSparc.bin`**.
4. Press **Enter**.
5. At the Welcome screen, click **Next**.
6. On the next screen, which displays the location of the Uninstall program, click **Next**.
7. On the next screen, which displays the installation summary, click **Next** to run the installation. The Installation Tool performs the following:

- Creates a backup directory and moves the existing web client connector files to that directory.
- Copies the new web client connector files to the proper directories.

- Copies the files from the Java folder to the proper directories.
- 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/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/7.3.2/WebConnector/Log/install.log LIST OF ERRORS AND WARNINGS

8. Click **Finish**.
9. If the installation is unsuccessful, run the Uninstall program. Correct the errors and re-run the Installation program.

AIX installation procedures

AIX installation prerequisites

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

1. Ensure that all IC components are stopped as explained in Stop Avaya Agent Web Client.
2. Change directory to $AVAYA_IC73_HOME/lib.
3. At the command line, type the command: **`slibclean`**.
4. At the command line, type the command: **`fuser -k lib*12d*.a`**.

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

   `fuser lib*12d*.a`.
5. 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 line:

   fuser lib*.so

   No process IDs should be displayed in the results after running this command. However, even if one process ID is displayed in the results, then you need to restart the AIX machine.
6. After performing the earlier steps, install AAWC on the AIX platform.

AIX installation

Perform the following steps on the AIX machines that are running the Avaya Agent Web Client.

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

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

2. At the command line, navigate to the directory where you uncompressed the contents of the IC732AixWebConnector.tar file.
3. At the command line, type: ./setupaix.bin
4. Press **Enter**.
5. On the Welcome screen, click **Next**.
6. The next screen displays the location of the Uninstall program, click **Next**.
7. On the next screen which displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

- Creates a backup directory and moves the existing web client connector files to that directory.
- Copies the new web client connector files to the proper directories.
- Copies the files from the jre folder 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/7.3.21/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/7.3.2/WebConnector/Log/install.log LIST OF ERRORS AND WARNINGS

8. Click **Finish**.
9. If the installation is unsuccessful, run the Uninstall program. Correct the errors and re-run 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 7.3.2 release.

This component must be installed on the machine where the Avaya Agent Web Client package is installed, not the deployment machine.

This section includes the following topics:

Installation path procedures

The IC 7.3.2 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:

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, 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 machines that are running the Avaya Agent Web Client.

1. Go to the directory where you extracted the contents of the IC732WinWebClient.zip file.
2. Open the IC732WinWebClient folder and double-click on setupwin32.exe to start the installation program.
3. At the Welcome screen, click Next to continue.
4. On the next screen, which displays the location of the Uninstall program, click Next.
5. On the next screen, which displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

- Creates a backup directory and moves the existing web client files to that directory.
- Copies the web client files to the proper directories.
- 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\WebClient\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\WebClient\Log\install.log LIST OF ERRORS AND WARNINGS

\install.log	

6. Click **Finish**.
7. If the installation is unsuccessful, run the Uninstall program. Correct the errors and re-run the Installation program.
8. After successful installation, manually merge the customization files, if any.
9. Generate the war file and deploy on to the webconnector machines.

Note: To generate webclient.war file and deploy on Windows/AIX/Solaris Webconnector machines, please refer to "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 7.3.2 Administration and Design component. Only the Windows platform supports the IC 7.3.2 Administration and Design component.

Windows installation procedures

Perform the following steps on each machine where administration tools are installed.

1. Stop the IC Manager, Avaya Database Designer, and Workflow Designer applications if they are already running.
2. Go to the directory on the central server where you extracted the contents of the IC732WinAdmin.zip file.
3. Copy the IC732WinAdmin folder to the machine 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 machine.
4. Open the IC732WinAdmin folder on the machine from which you want to install.
5. Double-click the setupwin32.exe to start the installation.
6. On the Welcome screen, click **Next**.
7. On the next screen, which displays the location of the Uninstall program, click **Next**.
8. In the pop-up window that prompts, Please log out from IC Manager, click **Continue**.
9. On the next screen, which displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

- Creates a backup directory and moves the existing admin files to that directory.
- Copies the new admin files to the proper directories.
- Registers the new .ocx and .dll files.
- Installs the Uninstall program.
- Displays the results of the installation.

If installation is successful, the system displays:	If installation is unsuccessful, the system displays: ALERT! Installation failed. Please fix these errors

Installation was successful. No errors or warnings were generated. Complete log messages are available at: ...\IC73\ICServicePacks\7.3.2\DesignAdmin\Log\install.log	and re-run the installer. The following errors or warnings were generated. Complete log messages are available at: ...\IC73\ICServicePacks\7.3.2\DesignAdmin\Log\install.log LIST OF ERRORS AND WARNINGS

10. Click **Finish**.
11. If the installation is unsuccessful, run the Uninstall program. Correct the errors and re-run the Installation program.

Importing the sc.xml file

You must import the sc.xml file to fix configuration related issues in IC Manager. The sc.xml file is located in the folder where you unzipped the contents of IC732WinAdmin.zip file.

To import the sc.xml file:

1. Rename the existing file <AVAYA_IC73_HOME>\etc\sc.xml to <AVAYA_IC73_HOME>\etc\sc.xml.bak
2. Copy the new sc.xml file to <AVAYA_IC73_HOME>\etc.

Note: In case, if you have performed any customization in the existing "sc.xml" file, merge that changes from "sc.xml.bak" to the new "sc.xml" file you copied in step 2 above.

3. Log on to IC Manager as Admin.
4. From the IC Manager, click **Manager** > **Options** > **Environment** tab.
5. Click the **Import Configuration** button.
6. From the **Open** dialog box, select the sc.xml file that you copied in step 2 above, and click the Open button.
7. 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.

Note: If you have merged any previous customization changes in the new sc.xml file, check the xml syntax for well-formedness and import the sc.xml file again.

Avaya Agent Rich Client installation

This section describes the installation procedures for the IC 7.3.2 Avaya Agent (rich client) component. Only the Windows platform supports the Avaya Agent installation.

Note: You can install the IC 7.3.2 Avaya Agent (rich client) component after all the other IC 7.3.2 FP components are installed and configured. You do not require stopping the IC Servers before installing the IC 7.3.2 Avaya Agent (rich client) component.

Installation procedures

Perform the following steps on each agent workstation.

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

2. Go to the directory on the machine where you extracted the contents of the IC732WinAgentClient.zip file.
3. Copy the IC732WinAgentClient folder to the machine 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 machine.
4. Open the IC732WinAgentClient folder and double-click on setupwin32.exe to start the installation program.
5. In the Welcome window, click **Next**.
6. The installation runs the Preinstall options that unregister the .ocx and .dll files that are patched in this installation.
7. On the next screen, which displays the location of the Uninstall program, click **Next**.
8. In the pop-up window that prompts, Please logout Avaya Agent, click **Continue**.
9. On the next screen, which displays the installation summary, click **Next** to run the installation.

The Installation Tool performs the following:

- Creates a backup directory and moves the existing agent files to that directory.
- Copies the new agent files to the proper directories.
- Registers the new .ocx and .dll files.
- 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\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\7.3.2\AvayaAgent\Log\install.log LIST OF ERRORS AND WARNINGS

10. Click **Finish**.
11. If the installation is unsuccessful, run the Uninstall program. Correct the errors and re-run the Installation program.
12. If the installation is successful, reboot the agent machine.

Avaya Agent installation in silent mode

On the Windows platform, you can also run the IC 7.3.2 Avaya Agent installation in silent mode. The silent mode option is for Avaya Agent installations on multiple machines.

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, re-run the same installation in silent mode on another machine using the inputs from this text file.

Record mode

To run the installer in record mode:

1. Click **Start** > **Programs** > **Accessories** > **Command Prompt**.
2. Go to the package directory where the contents of the FP installer are extracted.
3. At the command prompt, type: **`setupwin32.exe -options-record <AbsolutePathOfFile.ext>`**.

   Note: The <AbsolutePathOfFile.ext> is a placeholder for the qualified complete file name, where "AbsolutePathOfFile" is the name of the file and "ext" is the file extension.
4. Press **Enter**.
5. Complete the installation using the information in Avaya Agent Rich Client installation. The installer creates the <AbsolutePathOfFile.ext> file containing all of your inputs.

Silent mode

To re-run the installer in silent mode:

1. Copy the `<AbsolutePathOfFile.ext>` file to the machine where you want to install.
2. Click **Start** > **Programs** > **Accessories** > **Command Prompt**.
3. Go to the package directory where the contents of the FP installer are extracted.
4. At the command prompt, type:

   setupwin32.exe -options `<AbsolutePathOfFile.ext>` -silent

   For example, setupwin32.exe -options "D:\temp\SP732Silent.opt" -silent
5. Press **Enter**.

   The installation runs (without a GUI) using the <AbsolutePathOfFile.ext> file for your inputs.

Start IC servers

After you complete the Avaya IC 7.3.2 Server installation program, delete all the files under the tomcat cache path `AVAYA_IC73_HOME\tomcat\\work\Catalina\localhost\rlmanager\org\apache\jsp`. Restart the IC servers by running both of these tools in the following order:

Avaya IC Admin Utility

To restart the ORB server using the Avaya IC Admin Utility on the server machine:

1. At the command prompt, navigate to the following directory:
   - Windows: ...\IC73\bin
   - Solaris and AIX: .../IC73/bin
2. Type the following command:
   - Windows: icadmin so
   - Solaris and AIX: ./icadmin so
3. Press **Enter**.

IC Manager

In IC Manager, you must restart the IC servers individually and in the proper order. Before you begin, run the procedures described in Avaya IC Admin Utility restart the ORB server.

To restart IC servers in IC Manager:

1. Click the Server tab and select the server to be restarted. The following table lists the order in which to start the servers.
2. Click the **Start Server** button.

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	IC Email 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

On the Windows platform, after you complete the Avaya IC 7.3.2 Server installation program, all the IC Services need to be started if they are not already started.

Windows

The steps given in this section are for the Windows platform.

To start the IC Services:

1. Start the Windows Services application.
2. Start any of the following services that are not already started (some may 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 Voice Media Manager
- Avaya SDK Services
- Avaya Business Advocate Component Manager
-

Solaris and AIX

The steps given in this section are for the Solaris and AIX platforms.

To start the IC Services:

1. Move to the .../IC73/bin directory.
2. For ICM:
   a) At the command prompt, type: **`./icm.sh start`**.
   b) Press **Enter**.
3. For CIRS:
   a) At the command prompt, type: **`./cirs.sh start`**
   b) Press **Enter**.
4. To start multiple Tomcat instances:
   a) At the command line, type: **`./ictomcat.sh start all`**
   b) Press **Enter**.
5. To start single Web application:
   a) At the command line, type: **`./ictomcat.sh start <servicename>`**
   b) Press **Enter**.
6. 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
7. For IBM http Web Server

a) Change the directory to: AVAYA_IC73_HOME\IC73\bin

b) At the command line, type: **`./httpserver.sh start`**

c) Press **Enter**.

Start the VMM service (Solaris only)

If you host your Avaya IC servers on Solaris and have the VMM service configured, you must restart the VMM setup service for Voice Chat. The VMM setup service configures the VMM to start automatically.

You only must perform this step if you host your Avaya IC servers on Solaris. Do not perform this step if you host your servers on Windows machines.

To run the VMM setup script and start the VMM on Solaris:

1. Navigate to the following directory: **`IC_INSTALL_DIR/IC73/bin`**.
2. At the command line, type: **`./vmm_setup start`**.
3. Press **Enter**.

Start Avaya Agent Web Client

After you run the IC 7.3.2 installation, you can start the Avaya Agent Web Client component by handling the javaw process.

To start the javaw process

1. Click **Start** > **Run** to open the command prompt.
2. Change the directory to: AVAYA_IC73_HOME \bin.
3. Execute the following commands:

Operating System	Procedure
Windows	To start: **`aawcclient.bat start`**
Solaris and AIX	To start: **`./aawcclient.sh start`**

Configurations

IC 7.3.2 Feature Pack Configuration

Configuration for WebLM

Perform the following steps on the machine where WebLM server is installed.

1. Stop Tomcat server (Stop the WebLM service)
2. Before upgrading the WebLM server, backup the set of files as described in the table above.

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. E.g 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.

3. Delete the <AVAYA_IC73_HOME>/tomcat/webapps/WebLM folder.
4. Start the tomcat server.

   This will extract the new WebLM.war file from the IC732 server installer of respective platforms (AIX,

Solaris, and Windows)

5. Stop the tomcat server.
6. Restore/Overwrite the above set of files in the respective file/folder location.
7. Locate the server.weblm.xml file normally located under the <AVAYA_IC73_HOME>/tomcat/conf folder.
8. Open this file using any editor (e.g. Notepad, Textpad, vi – based on OS used).
9. Go to end of file and add Connector tag for port 52233 which will be used as the HTTPS port for WebLM. The following element should be added before the element "</Service>":

   Note: As per the Licensing Conformance Requirements [125163-M-850], licensed products shall utilize port 52233 for HTTPS communication with WebLM server.

   Configuration for Tomcat Installation without APR **:

   <Connector acceptCount="100" clientAuth="false" disableUploadTimeout="true" enableLookups="false" keystoreFile="${catalina.base}/webapps/WebLM/WEB-INF/weblmserver.p12" keystorePass="password" SSLEnabled="true" keystoreType="PKCS12" maxHttpHeaderSize="8192" maxSpareThreads="75" maxThreads="150" minSpareThreads="25" port="52233" scheme="https" secure="true" sslProtocol="TLS" ciphers="SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA,SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SHA,SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA,TLS_KRB5_WITH_3DES_EDE_CBC_MD5,TLS_KRB5_WITH_3DES_EDE_CBC_SHA,TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA,TLS_DHE_DSS_WITH_AES_128_CBC_SHA,TLS_DHE_DSS_WITH_AES_256_CBC_SHA,TLS_DHE_RSA_WITH_AES_128_CBC_SHA,TLS_DHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA"/>

   Configuration for Tomcat Installation with APR**:

   <Connector acceptCount="100" clientAuth="false" disableUploadTimeout="true" enableLookups="false" SSLPassword="password" SSLEnabled="true" maxHttpHeaderSize="8192" maxSpareThreads="75" maxThreads="150" minSpareThreads="25" port="52233" scheme="https" secure="true" sslProtocol="TLS" SSLCipherSuite="ALL:!ADH!RC4 -IDEA:!LOW:!SSLv2:!EXPORT40!EXPORT56" SSLCertificateFile="${catalina.base}/webapps/WebLM/WEB-INF/weblm.crt" SSLCertificateKeyFile="${catalina.base}/webapps/WebLM/WEB-INF/weblm.key"/>

   Note:

   This is assuming that WebLM is deployed in <tomcat_installation_dir>/webapps folder. Be careful while doing a copy paste from this document into the server.xml file. Ensure that the valid quotes are copy pasted in the server.xml file.

10. For the Connectors on port 8080 and 8009, update the value of attribute “redirectPort” from (default) 8443 to 52233.
11. Start Tomcat/WebLM service and access WebLM
12. In the Web browser, enter the URL of the WebLM server in the following format:

Error! Hyperlink reference not valid.

Database Configuration for IC 7.3.2 Feature Pack

Note: This section is mandatory for IC 7.3.2 FP even if Email Template feature is not used.

Pre-requisites:

Install IC 732 FP before applying the following configuration changes.

Database Configuration

Summary of Configuration changes:

This service pack ships **ccq_732.adl and repository_732.adl** file in $AVAYA_IC73_HOME/design/CallCenterQ and $AVAYA_IC73_HOME/design/repository folders respectively. If you have made any customizations in these files present with 7.3 RTM installer, you need to manually merge your customizations with ccq_732.adl and repository_732.adl before performing database administration.

The database can be re-configured with the following steps

- Import new properties TemplateDownload and StatusDownload
- Update database schema
  - repository.adl Database table changes
  - ccq.adl Database table changes
  - Reconfigure the Database

Import new properties TemplateDownload and StatusDownload

a. Log on to the IC732 Database Design machine
b. Go to command prompt
c. Change directory to repository data

```
> cd /D %AVAYA_IC73_HOME%\design\repository\data
```

d. Execute the **import_properties.bat** command by passing arguments **<Admin_Name>** & **<Admin_Password>**
for example:

```
D:\Avaya\IC73\design\repository\data>import_properties.bat Admin admin1
IcImportTool
Version: 7.3.1.3
--------------------------------------------------
```

```
Converting CSV files to XML

Adding PropSection entries to Intermidiate XML
...
Adding Property entries to Intermidiate XML
...
Adding PropertyValue entries to Intermidiate XML
...
Adding PropertyInstance entries to Intermidiate XML
...
Saving Intermidiate XML to Disk
Done creating D:\Avaya\IC73\etc\prop.xml
Vesp login in progress
Vesp login successful
...
End property import
```

e. For more details about success or failure please check the **<AVAYA_IC73_HOME>\logs\General_Admin.log** file. Below is the log snippet of above command from **General_Admin.log** file.

```
  17:28:46     Info: main Unknown- Section 'Agent/Desktop/Resources' already
exists

    17:28:46     Info: main Unknown- Property: MyResourcesEnabled alreadt exists
in Section 'Agent/Desktop/Resources

    17:28:46     Info: main Unknown- PropInstance 1 Already exists for Property
MyResourcesEnabled Section Agent/Desktop/Resources

    17:28:46     Info: main Unknown- NEW: Property: TemplateDownload created in
Section 'Agent/Desktop/Resources

    17:28:46     Info: main Unknown- NEW: Value All, Description Agent is able
to view and use templates from all email template folders. Added to property
TemplateDownload Section Agent/Desktop/Resources

    17:28:46     Info: main Unknown- NEW: Value Selective, Description Agent is
able to view and use only the email templates from the folders mapped to agent's
workgroup. However, agent can switch the view to use templates from all the
folders. Added to property TemplateDownload Section Agent/Desktop/Resources

    17:28:46     Info: main Unknown- NEW: Value Restrictive, Description Agent
is able to view and use only the email templates from the folders mapped to
agent's workgroup. The agent cannot switch to any other view. Added to property
TemplateDownload Section Agent/Desktop/Resources

    17:28:46     Info: main Unknown- NEW: PropInstance All Added for property
TemplateDownload in Section Agent/Desktop/Resources

    17:28:46     Info: main Unknown- NEW: Property: StatusDownload created in
Section 'Agent/Desktop/Resources

    17:28:46     Info: main Unknown- NEW: Value All, Description Agent will be
able to view and use resolve status from all the folders. Added to property
```

```
StatusDownload Section Agent/Desktop/Resources

    17:28:46     Info: main Unknown- NEW: Value Restrictive, Description Agent
will be able to view and use only the resolve statuses from the folders mapped
to the agent's workgroup. Added to property StatusDownload Section
Agent/Desktop/Resources

    17:28:46     Info: main Unknown- NEW: PropInstance All Added for property
StatusDownload in Section Agent/Desktop/Resources

    17:28:46     Info: main Unknown- Section 'Agent/Desktop/Spelling' already
exists
```

Update Database Schema

Changes in repository.adl

Added a new table **qem_folderworkgroup** in **q_qem** tableset.

The database ccq.adl has following schema changes

i. Added new COLUMNS in **qem_folder**, **qem_resolvestatus**, and **qem_template**

(Existing Table Name) {Newly Added Columns}

```
(qem_folder) {disabled, lastmodifiedby, inherit}

(qem_resolvestatus) {lastmodifiedby, lastmodified}

(qem_template) {lastmodifiedby, lastmodified}
```

ii. Added new TABLE **qem_folderworkgroup**

(New table Name) {Columns}

```
(qem_folderworkgroup) {pkey, folder_id, workgroup_id}
```

iii. Defined TABLESET **q_qem** by adding tables to it

(Newly added Table Names to TABLESET q_qem)

```
(qem_folderworkgroup, workgroup, employee)
```

iv. Defined MODULE **q_tr_qem** by adding new RELATION to it.

(Newly added RELATION) {TYPE} {FROM TABLES}

NEW RELATION NAME	TYPE	TABLES
qem_template_employee	1: Many	qem_template, employee
qem_resolvestatus_employee	1: Many	qem_resolvestatus, employee

qem_folder_employee	1: Many	qem_folder, employee
qem_folder_qem_folderworkgroup	1: Many	qem_folder, qem_folderworkgroup
workgroup_qem_folderworkgroup	1: Many	Workgroup, qem_folderworkgroup
qem_folderworkgroup	Many: Many	**NODES:** qem_folder, qem_folderworkgroup, workgroup **EDGES:** qem_folder_qem_folderworkgroup, workgroup_qem_folderworkgroup

Reconfigure the database

If you have made any customizations in these files present with 7.3 RTM installer, you need to manually merge your customizations with ccq_732.adl and repository_732.adl before performing the following steps.

1. Log on to the IC732 Database Design machine.
2. Launch the Database Designer application.
3. Using **File** -> **Open** menu option select the file "**...\<AVAYA_IC73_HOME>\design\repository\repository.adl**
4. Reconfigure the database and Generate Windows Application using the normal reconfiguration procedure (Please refer Admin guide for detailed steps).
5. Close the ADL file using **File -> Close** menu option.
6. Using **File** -> **Open** menu option select the file "**...\<AVAYA_IC73_HOME>\design\CallCenterQ\ccq.adl**
7. Reconfigure the database and Generate Windows Application using the normal reconfiguration procedure (Please refer Admin guide for detailed steps).

Creating or Reconfiguring RL Manager service

Perform the only if RLManager is configured or you wish to configure a new RLManager service.

a. Import <AVAYA_IC73_HOME>\etc**sc.xml** in ICManager
b. Ensure that RL Manager service (Avaya IC Email Template Management Service 7.3) is not running
c. Open the **IC Config Tool** on the server where RL Manager is deployed (or needs to be deployed)
d. **Enable** “Configure Email Template Administration” if it is not already enabled.
e. If “Configure Email Template Administration” is already enabled, disable it and click on “**Apply Settings**”. This will **remove** the Email Template Administration Service. You will be prompted to restart the server. Please do so and start configuration from step ‘b’.

f. Enter the **username** of DCOBridge user against “Email Template Administrator Login” (example: “dcobridge1”).
g. Enter the **password** of DCOBridge user by clicking the “…” button in front of “Email Template Administrator Password” (example: “dcobridge1”).
h. Click on “**Apply Settings**”.
i. Wait for a message confirming successful deployment of RL Manager Service.
j. Click on “**Exit**”

Web.xml configuration parameters

Table below describes additional parameters to control message delivery to ICEmail servers.

Sr. No.	Configuration parameter	Default value	Mandatory?	Description
1	rlmanager.vesp.request.rejectchangerecordcounter	5	No	Controls how many times particular change record should be resent to ICEmail server in case of an error. In case ICEmail server faces DB error, RLManager will retry to send same record. This could end up in a loop if ICEmail server doesn’t recover from Database error. Use this configuration parameter to control how many times RLManager should try 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 will receive CTI exceptions.
3	rlmanager.vesp.request.retrytime	180000 milliseconds	No	RLManager uses a queue to deliver change record to ICEmail server. In case RLManager has to retry sending a change record, this record is pushed in this

				queue. This configuration parameter controls on how frequently retry of such change records are 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 (which refresh everything in ICEmail server).

ICEmail configuration (optional)

Not to recreate Template data on GenericUpdate

ICEmail clears it's cached template trees and recreates its in-memory data on a Generic Update.This the default behavior.

To turn off recreating in-memory data on a Generic Update, set TemplRecreateGenUpdas 0 on the configuration tab on ICEmail from ICManager.

A value of 1 will retain the default behavior.

Enable logging of JSON tree sent to agent (optional)

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

Security configurations for Website:

The security fixes contain changes to the website configuration. Hence, reconfiguration is required on 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 may be better to rerun the configtool for website, customers may follow a manual approach to the same in case there are configuration changes done in web.xml file.

When Config Tool is run, it makes necessary changes the web.xml. For manual changes, following steps can be followed:

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 (refer to 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) If making changes on the server hosting the Admin site, also enable the SQL Injection filter by removing the surrounding comment tags.
3) 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 (refer to 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/changes are recommended for improving the security of Avaya IC application.

- Always deploy Public and Administration website on separate servers
- Keep the server hosting the Administration website inside of the firewall
- Always enable HTTPS and disable HTTP for webserver and the tomcat application Turn off directory browsing for the website on the webserver
- Turn off Anonymous access to website related files/folders by the webserver application

Note: Recommendations #1 & 2 would help secure IC website against the following vulnerability (wi01123999):

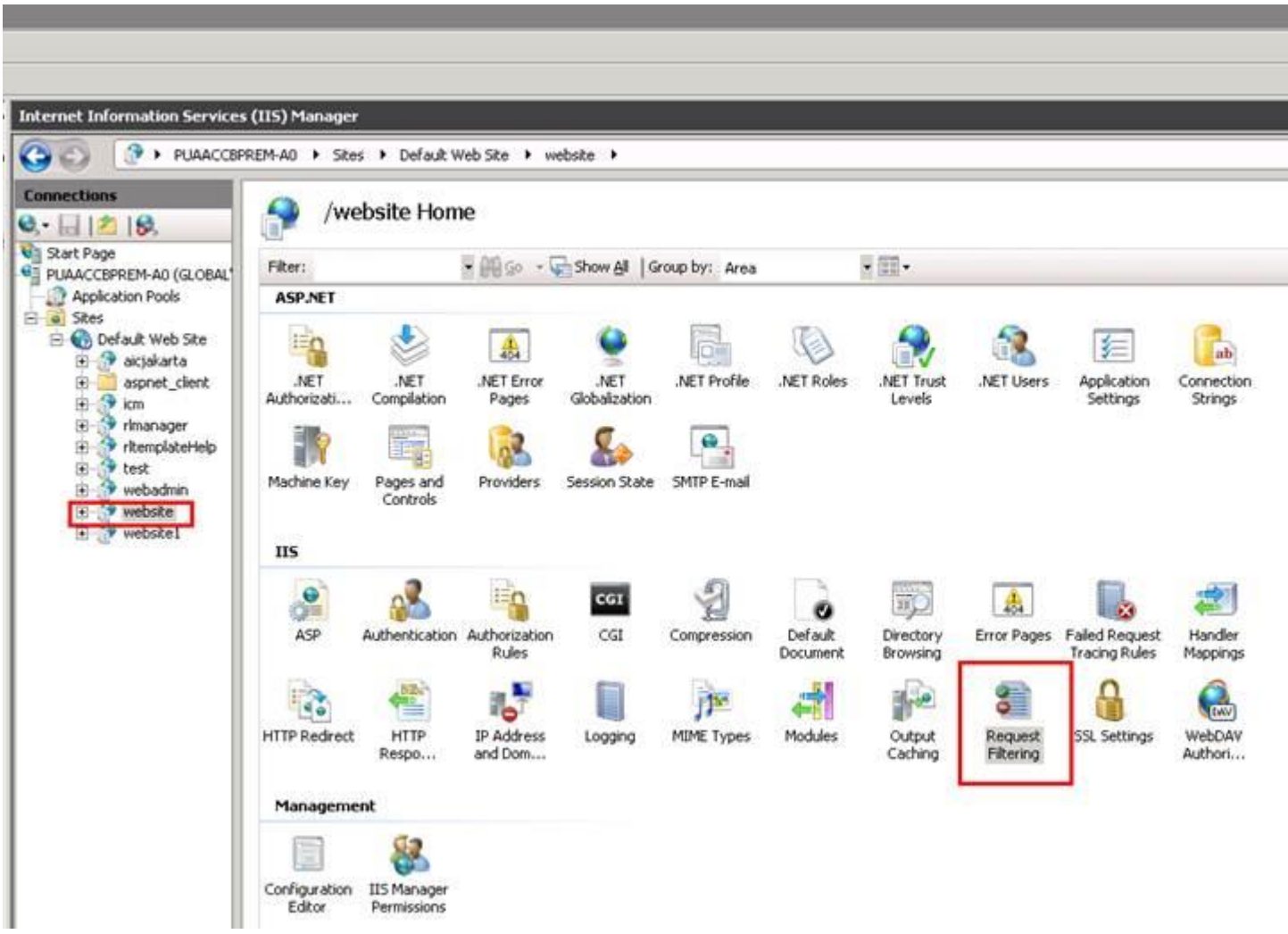
A malicious user that can guess the path to the web interfaces can potentially guess or brute force a password to gain administrative control of the application.

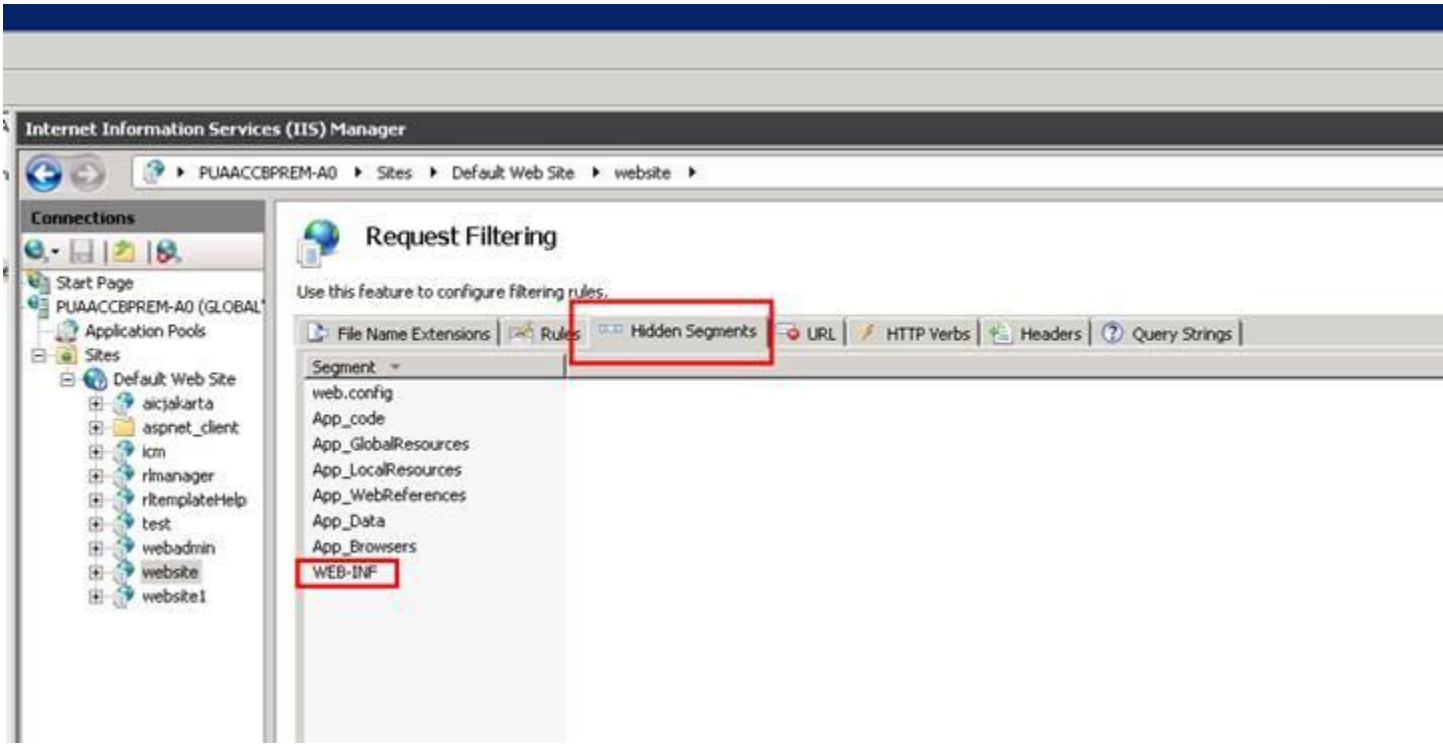
Deployment of AAWC:

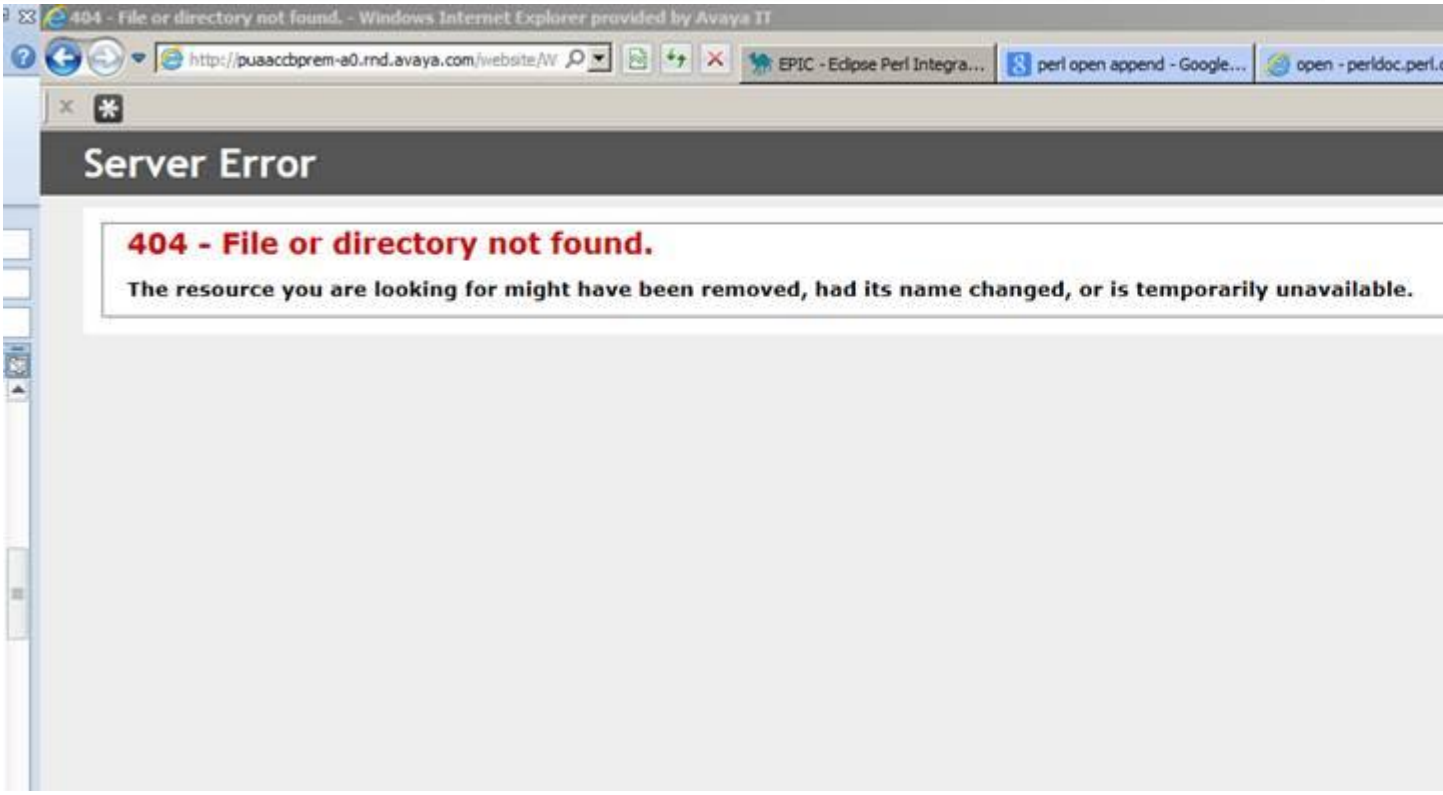
1. Generate the webclient.war file by running the "wargenerater.bat" file available in the <AVAYA_IC73_HOME> folder.
2. Copy the generated war file to the AAWC Connector machine.
3. Stop the AAWC application.
4. Deploy the newly generated war file on tomcat, by copying the war file to <AVAYA_IC73_HOME>\tomcat\Avaya\war folder
5. Delete the “avaya” or “avaya#agent” present at location <AVAYA_IC73_HOME>\tomcat\webapps\
6. Delete the “avaya_agent” folder present at
7. <AVAYA_IC73_HOME>\tomcat\work\Catalina\localhost\
8. Start the AAWC 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:




Internet Information Services (IIS) Manager
PUAACCBPREM-A0 ▸ Sites ▸ Default Web Site ▸ website ▸
Connections
Start Page
PUAACCBPREM-A0 (GLOBAL
Application Pools
Sites
Default Web Site
aicjakarta
aspnet_client
icm
rlmanager
rltemplateHelp
test
webadmin
website
website1
Request Filtering
Use this feature to configure filtering rules.
File Name Extensions
Rules
Hidden Segments
URL
HTTP Verbs
Headers
Query Strings
Segment
web.config
App_code
App_GlobalResources
App_LocalResources
App_WebReferences
App_Data
App_Browsers
WEB-INF



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 don't really need this header in case of content without frames, so this should not really be an issue.

Configuration for AUX Reason code for RONA:

TS does 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.

This feature is supported with AARC, AAWC, SDK and not supported with 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 pre-configured 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.

Note: This is applicable to IC Business Advocate configuration. In case of non-BA systems, these configurations would not be used. System should not be set to use CM RONA as well as IC RONA.

Exit_reason for RONA calls:

TS sets the container exit_reason to either “rerouted” or “normal” for RONA calls and this makes it difficult to report RONA calls in IC reporting

The change would be consistent with other media (email and chat) and the exit_reason would be “RONA” for both Advocate and Non-Advocate systems. Customers can now query the exit_reason to determine the RONA calls. There are no configuration changes needed for this feature to work.

Configuration for Inactivity timeout for Chat Disconnect:

A provision has been added to the OOTB IC public website wherein the ongoing live chat between the customer and the Agent will get 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

Procedure to add the metadata properties for the above feature.

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 secs) determines the time duration for which a inactivity warning messsage would be displayed to the customer.Default is 60 secs.
- The second value (in secs) determines the duration for which the countdown timer changes color to signify that chat disconnection time is closing upon.Default is 10 secs.
- 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.

- Click Add Metadata.
- 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 JoinUS customer.Valid values are true/false.

  Tenant Property(checked)

10. In case the above tenant values requires to be changed , then it can be changed from the IC Multitenant administration page.

- Traverse to http://<server_name>/website/admin/index.jsp page and select "IC website Multi Tenant Administration"
- Click Tenant Properties and select the appropriate tenant.
- Click "chat".
- Search for following meta data chat property and make appropriate changes to their values.
  a. chat.htmlclient.customer.inactivitytimer.enabled
  b. chat.htmlclient.customer.inactivity.totaltime
  c. chat.htmlclient.customer.inactivity.countdowntime
  d. 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" as well.

14. 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 would be disconnected after the customer inactivity time crosses the disconnect interval
- This feature is only available for chat only and doesn't support the case where the customer is simultaneously using cobrowse/collaboration. In such a scenario the customer still has to press in any key to keep the chat active.
- The above feature is useful only in case where customer wants a disconnection feature on the customer end and customer doesn't use the collaboration/cobrowse feature.

The ResetScriptIteration setting for WACD

Please refer to IC 7.3.1 Service pack configuration section.

Note:

This is applicable if IC is upgraded from IC 7.3 or IC 7.3.1 SP.

IIS-Tomcat Redirector configuration

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 this service pack

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. Note the application pool used.
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 their status table after the configuration. The Tomcat Redirector and the Tomcat server will 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 will not be 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 should set the Tomcat connectionTimeout parameter to 600000.

The Tomcat Redirector has been upgraded in this service pack and consequently some of the directives used in the Tomcat Redirector configuration files have changed. For details on deprecated directives, refer to: http://tomcat.apache.org/ connectors-doc/reference/workers.html

Allowing non-RFC compliant emails to be processed by AIC

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 will remain on the email server and the Poller server will alarm every polling interval about this email until it is cleared from the mailbox. To disable or enable RFC compliance, a new configuration value for the Poller server has been provided. For more information, refer to wi00845454.

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)

4. Log in to ICManager using admin account.
5. Click the **Server** tab.
6. Double-click the **Poller server**.
7. Click the **Configuration** tab.
8. Add a new Couple with name: DisableEmailAddressRFCCheck.
9. 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 will be bounced by the Poller server's SPAM plugin 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.

10. Click **OK**.
11. 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 will be 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.
5. 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 will be used as a substitute address.

6. Click **OK**.
7. Restart the Poller Server.

New Connection properties for SDK login issue

SDK agents cannot login after network issue**.** To resolve this issue, following properties can be configured 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.

IC 7.3.1 Service Pack Configuration

Avaya Agent Web Client (AAWC) Configuration

Perform the following steps on the windows machine where AAWC is installed:

1. Create the new webclient.war file using wargenerator.bat on WebClient machine.
2. Redeploy the newly created webclient.war file on WebClient Connector machine. For more information, refer IC 7.3 Installation and Configuration.pdf.

Note: To generate webclient.war file and deploy on Windows/AIX/Solaris Webconnector machines, refer to "IC7.3 Installation and Configuration guide" in Avaya Support Site http://support.avaya.com

Avaya Agent Rich Client (AARC) Configuration

Perform the following steps if WACEngine_PerformConsoleAction.qsc file is not updated as per below steps on the Design and Admin machine for Windows:

1. Exit the Avaya Agent if it is running.
2. Backup the following files:

   ...\IC73\design\QConsole\WACEngine_PerformConsoleAction.qsc

3. Locate the following in the script.

```
Else
    If Len(sHTTPExecutable) = 0 Then
        lReturn = ShellExecuteA(0, "open", sParameter, "", "", 1)
    Else
        lReturn = Shell(sHTTPExecutable, ebNormalFocus)
        lReturn = ShellExecuteA(0, "open", sParameter, "", "", 1)
    End If
End If
```

4. Replace the middle IF-Else-End If statements with a single line so that it looks like as shown.

```
Else
    lReturn = ShellExecuteA(0, "open", sParameter, "", "", 1)
End If
```

5. Start the Avaya Database Designer.
6. Push the scripts to the database.

SDK Server Configuration

You need to manually replace the IC SDK Server files installed on the Windows, Solaris, and AIX platforms if

IC SDK Server is installed and configured.

Perform the following configuration steps to replace the files:

1. Stop the IC SDK Service, if running, on the applicable platforms using following:

Windows:

- Start the Windows Services application.

2. Stop the IC SDK Service.

Solaris/AIX:

- At the command line, type: **./ictomcat.sh stop SDK -force**

3. Press **Enter**.

4. Backup the following files from the ..\IC73\sdk\server\icsdk\WEB-INF\lib\ location and Manually copy the following files from the IC 7.3.2 Service Pack to the ..\IC73\sdk\server\icsdk\WEBINF\ lib folder:

- avaya-ic-services.jar
- avaya-ic-webui.jar
- avaya-ic-sdk-common.jar
- avaya-ic-sdk-server.jar
- avaya-common.jar
- avayai ccommmon.j ar
- avayaaut h.j ar
- avaya-i c-sdk-sampl e.j ar
- avaya-i c-appl i cat i on.j ar
- WebAgent .j ar

5. Backup following files from ..\IC73\sdk\design\dotnet\lib folder and manually copy the following files from sdk folder of IC 7.3.2 Service Pack to the ..\IC73\sdk\design\dotnet\lib folder:

- AvayaICSDKClient.dll
- AvayaICSDKClient.pdb
- AvayaICSDKClient.xml
- Com.Avaya.Util.dll
- Com.Avaya.Util.Messaging.dll
- Com.Avaya.Util.Messaging.pdb
- Com.Avaya.Util.pdb
- CSharptester.pdb

6. Backup following files from sdk\design\dotnet\sample\bin folder and manually copy the following files from sdk folder of IC 7.3.1 Service Pack to the ..\IC73\sdk\design\dotnet\sample\bin folder:

- AvayaICSDKClient.dll
- AvayaICSDKClient.pdb
- AvayaICSDKClient.xml
- Com.Avaya.Util.dll
- Com.Avaya.Util.Messaging.dll
- Com.Avaya.Util.Messaging.pdb
- Com.Avaya.Util.pdb
- CSharptester.exe
- CSharptester.pdb

7. Backup the following folders from the specified folder location and manually copy the following from the IC 7.3.1 Service Pack to the specified folder location:

- The Controller and UI folders from sdk\design\dotnet\sample\src\Com.Avaya.Ic.Sdk.Sampleclient.
- The MSDN folder from sdk\design\dotnet\doc.
- The Doc folder from sdk\design\java\doc.
- The src folder from sdk\design\java\sample.

8. Ensure that the newly copied files have the same read/execute permissions as the backed-up files.

9. Start IC SDK Service on the applicable platforms:

Windows:

i. Start the Windows Services application.

ii. Start Avaya SDK Services

Solaris/AIX:

i. At the command line, type: **./ictomcat.sh start SDK**.

ii. Press **Enter**.

Optional Security Configuration for IC Public Website for Modern day browsers

Note: These changes are not applicable to IC 7.3.2 SP and onwards.

Modern day browsers like IE8, IE9, Chrome 21, and so on 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 machines where website is installed. This is applicable for all platforms. If the admin and public websites are configured on separate machines, perform this for the public website.

1. Stop website service.
2. Browse to the following folder on the machine 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

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>sqliByPassURLPattern</param-name>

This parameter indicates which all URL patterns of the admin website needs to be bypassed for detection of SQLI attacks. These admin pages URL with the listed patterns, when detected, would only be checked against the "sqlHTTPAttackString" parameter values.

- <param-name>sqlHTTPAttackString</param-name>

The URLs, which are mentioned as part of the "sqliByPassURLPattern" init parameter, would only be tested for these HTTP SQL attack strings.

Perform the following steps on the machines where website is installed. This is applicable for all platforms. If the admin and public websites are configured on separate machines, perform this for the admin website.

1. Stop website service.
2. Browse to the following folder on the machine 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.

UTF-8 Encoding for outgoing emails from WebAgent

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, a 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 has been 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 will be 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 machine, 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’.

Log Collector Configuration

1. Perform these steps only if your setup had Log Collector configured to collect the log files prior to the installation of SP 7.3.1. Close all instances of LogCollectorClient that may be running on your Design and Admin machine.
2. Deleting existing LogCollector instances:
   a. Log in to IC Manager as Admin.
   b. Stop all instances of LogCollector server.
   c. Delete all instances of LogCollector server.
3. Importing the sc.xml file

   Perform the following steps on Design and Admin machines:

   a. Log in to IC Manager as Admin.
   b. From the IC Manager, click **Manager > Options > Environment tab**.
   c. Click the **Import Configuration** button.
   d. From the Open dialog box, select the sc.xml file and click the **Open** button.

e. If the file is successfully validated, the validate sc.xml dialog box displays a Successfully Validated message.

f. If the validation is unsuccessful you will get an xml parsing error. In this case, address the issues causing the error and perform the steps from 3.c again.

Note: If you have merged any previous customization changes in the new sc.xml file, check the xml syntax for well-formedness and import the sc.xml file again.

Siebel AICD Server Logging

Siebel AICD logging is enhanced to allow configuring file count and file size. These parameters are configured in the AICD.ini file. Follow the steps below for increasing the log file size or log file count.

Steps to increase log file size and log file count:

1. Shutdown the Communications Session Manager component from the Siebel Server Administration screen, if it is already running.
2. Open the AICD.ini file from Siebel Server's bin directory 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
```

Save and close the AICD.ini file.

4. Start the Communications Session Manager component from the Siebel Server Administration screen.

The default values used when these parameters are not configured are:

- `FileCount = 2`
- `FileSize = 2000000`

Website Logging

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 will continue 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 , i.e. <website_context_global_name>_debug.log. Refer to the IC 73 Installation and Configuration guide on how the website_context_global_name is specified. It must be the same as dsObject Name as specified in web.xml file of website.
3. The maximum log file size specified as part of the ICManager 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

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

Following is the summary of changes:

1. A 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 the ‘Submit Query’ button 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 the ‘Submit Query’ button 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 will display 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.
        i. The default value is 200. This is can be customized to a different value between 1 and 1000.
        ii. Any value less than 1 will be treated as 200 (default)
        iii. 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.
        i. Default value is 200 which is set via DefaultNTaskID
        ii. If LastNTaskID <=0 set LastNTaskID=DefaultNTaskID and if LastNTaskID>MaxRecord then set LastNTaskID=MaxRecord
        iii. If NTaskID is less than or equal to 0 , that is, invalid value that this value will be set to DefaultNTaskID
        iv. If admin set LastNTaskID which is greater than 1000, which is also invalid than LastNTaskID will be set to 1000
    c. To make the changes follow the given instructions:
        i. Stop the IC Website service on the IC server where website is deployed.
        ii. Navigate to the <AVAYA_IC73_HOME>\tomcat\work\Catalina\localhost\ directory and delete the folder ‘website’
        iii. Browse to “<AVAYA_IC73_HOME>\comp\website\admin\wtc\ and open transcript.jsp
        iv. Locate the following statement:

```
int defaultNTaskID = 200;
```

v. Change the value from 200 to any value between 1 and 1000.

vi. Save and close transcript.jsp.

vii. Start the IC Website service on the IC server where website is deployed.

Enhance the logging information of the WSCallback server

After applying the Service Pack:

1. Go to the <Avaya_IC_Home>\logs folder and delete the wscallback.log
2. Start the WSCallBack Server via the IC Manager.
3. For getting higher level debug logs change the log level to "4" via the IC Manager and editing the properties of the WSCallback server.(Debug tab).

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.

   Error! Hyperlink reference not valid..

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.

   Error! Hyperlink reference not valid.

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 directory location: %AVAYA_IC73_HOME%\comp\website\public folder.

9. 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. This cookie is set 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 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. See OOTB account.jsp for more information.

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.

This warning message can be customized 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]***	***Successive chat escalation , accessing the htmlclclient.jsp page directly [DOCKED/INVALID USER SESSION]***
none	Chat would be escalated.	Allow the chat to be escalated.	Allow the chat to be escalated.	The user would be redirected to escalate and hence account.jsp page.
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.	The user would be redirected to escalate and hence account.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.	If the user clicks the **Ok** button after the session expires then the chat escalation would fail eventually. Also accessing the htmlclient.jsp page directly after the user session has expired would redirect him to escalate and hence account.jsp

chat.htmlclient. redundant.action	***Successive chat escalation , accessing the htmlclclient.jsp page directly [UNDOCKED/INVALID USER SESSION]***	***Successive chat escalation , refreshing the chatframe.jsp page directly [UNDOCKED/VALID USER SESSION]***	***Successive chat escalation , refreshing the chatframe.jsp page directly [UNDOCKED/INVALID USER SESSION]***
none	Closing and opening the browser by waiting for session to expire, the user would be redirected to escalate and hence account.jsp page.	Allow the chat to be escalated.	Closing and opening the browser by waiting for session to expire , the user would be redirected to escalate and hence account.jsp page.
redirect	Closing and opening the browser by waiting for session to expire , the user would be redirected to escalate and hence account.jsp page.	User would be redirected to chatsessionexpire.jsp page.	Closing and opening the browser by waiting for session to expire , the user would be redirected to escalate and hence account.jsp page.
alert	If the user presses the Ok button after the session expires then the chat escalation would fail eventually. Also accessing the htmlclient.jsp page directly after the user session has expired would redirect him to escalate and hence account.jsp	A popup option would be displayed asking the user if he needs to escalate the chat. OK : Will escalate the chat again. Cancel : Will prevent the chat escalation.	If the user presses the Ok button after the session expires then the chat escalation would fail. Upon refreshing the chatframe.jsp page thereafter would redirect the user to chatsessionexpire.jsp page.

Note: For a CIRS case and when action = redirect, after the htmlclient.jsp is refreshed, the page is redirected to a JSP page specified by *website.pages.login* metadata attribute. This attribute points to *account.jsp* in OOTB website.

Web Form Design for Collaborative Form Filling

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 should 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 7.3.2 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>
```

Enabling *Refresh AddressBook* button for the ASIS server

When using native Siebel integration, if a new agent is added or an agent is deleted from ICManager, the ASIS server is not updated. Because of this, the changed agent information is not available until after restart of the ASIS server. 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 a new agent is added or an agent is deleted from ICManager, you can click the 'Refresh AddressBook' button in the ASIS server configuration to make the changed agent information available.

To activate the newly added 'Refresh AddressBook' button for the ASIS server, import the sc.xml file shipped with SP 7.3.1 or later by following the steps mentioned in 'Importing the sc.xml file' section in this document.

Changes to ICM Server and CIRS Log files

The ICM server log file name has been changed from icmlog.txt to 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 name has been changed from cirslog.txt to 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)' has been changed to '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 (i.e. 10-MB).

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.

Perform the following steps to set the maximum log file size for the ICM server, that is, for icmserver.log:

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. Refer to the IC 7.3 Installation and Configuration guide for more information. If you need to specify a different ICM value for the 'Maximum ICM Log size (KB)' parameter for different servers, then create a separate ICM configuration in IC Manager with unique global name.

ChannelWeightFactor for Business Advocate

Introduction

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 allows assigning 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:

1) ChannelWeightFactorVoice – for voice calls.
2) ChannelWeightFactorChat – for chat contacts.
3) 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.

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 of these 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 may 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 may 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.
   Weighted Contact Value = ChannelWeightFactorVoice * Number of voice calls currently serviced by the agent.
   Therefore, Weighted Contact Value for Agent1 = 2 * 1 = 2.
3) A new chat arrives and matches to Agent2.
   Weighted Contact Value = ChannelWeightFactorChat * Number of chat contacts currently serviced by the agent
   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

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

When this parameter is not configured, the default log file size is 10-MB. One backup file is created when the log file rolls over.

Using Lower case for Agent ID in custom SDK clients

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 have been 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.

Escaping Account creation / modification page of Admin website from SQL Injection Filter

Note: These changes are not applicable to IC 7.3.2 SP and onwards.

This configuration is required if:

- you use the IC database to store information about registered chat customers.
- you use the Create Account webpage of the Admin Website.

Perform these steps on the IC server where the website is deployed. The following procedure is for the Windows platform. The steps are the same for Solaris and AIX platforms except for the file and directory naming conventions and difference of method of starting and stopping the Tomcat web server.

1. Stop the IC Website. Refer to the IC Install and Configuration guide for the platform specific start and stop procedure.
2. Go to the %AVAYA_IC_HOME%\IC73\comp\website\WEB-INF location. Backup the web.xml file.
3. Open the **web.xml** file using a Text Editor.
4. Locate the filter by name, sqlAttackFilter, shown as <display-name>sqlAttackFilter</display-name>.
5. Within the same filter definition section, locate the element: <param-name>sqliByPassURLPattern</paramname>. In the parameter value, append aictuthaction=create and aicauthaction=edit to ByPass list as illustrated below:
    a. Old Value: <param-value>category=account,category=escalate,category=website</param-value>
    b. New Value: <paramvalue>category=account,category=escalate,category=website**,aicauthaction=create, aicauthaction=edit**</param-value>. The values must be in all lower case.
6. Change the parameter value irrespective of whether SqlAttackFilter is enabled or disabled.
7. Save and close this file.
8. Start the IC Website. Refer to the IC Install and Configuration guide for the platform specific start and stop procedure.

TwoStep Blind Transfer

Agent does a twostep blind transfer to an unmonitored VDN and the transfer does not get completed. Where the hold response is delayed and TS sends a TS.Transferinit response, before processing the hold event from CM fully. Hence, the call state is not yet updated fully in TS. In that time, the client sends a TS.TransferComplete request; TS seeing that primary call is not yet on hold, does not act on the Transfercomplete request and does not send the call merge request to CM. This leads to failure of blind transfer.

For Rich Client:

To fix this, the new parameter “TCDelay” is added in vtel.ini for Avaya Agent Rich Client.

TCDelay 0 #By default set it to 0

For AAWC/SDK:

Steps to Configure TCDelay:

1. Login to ICManager
2. Open the Group Manager window.
3. In IC Properties, navigate to Agent\Desktop\WebClient.
4. Provide appropriate value for TCDelay (default value is 0).

Note: The TCDelay property is used for TransferCancel delay as well. For more information, see *IC Administration* guide.

The ResetScriptIteration setting for WACD

With this feature, when the WACD server is restarted, WACD will maintain 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 email channel is not being used, 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:

5. If the new behavior of WACD server is required, perform the following steps for all WACD servers:
    - Login to ICManager
6. Go to the 'Server' tab and double click on a WACD server to edit its configuration.
7. Go to the configuration tab and add a new configuration parameter

- Name: ResetScriptIteration
- Value: 0

8. Click **OK** to save the WACD configuration
9. Gathering database information.

- Log in to ICManager.
- Open Tools menu and click on "IC Data Sources...".
- Once "IC Data Sources..." dialog opens expand "interaction_center".
- Click on ccqDBConnection.
- Note down Database Name and Database Server Values.

10. Update the w_script_details table
    - If the CCQ DB is of type SQL Server or DB2, execute the SQLDB2 Script given below
11. If the CCQ DB is of type Oracle execute the ORACLEDB script given below
12. After executing the query, from ICManager restart the WACD server.

    If the parameter is set to 1, WACD will behave as it used to, before the fix i.e. queue scripts will start from iteration zero. Priorities of tasks will be reset.

    If the parameter is set to 0, WACD will recreate 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 will be maintained as prior to restart.

13. 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 may 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;
```

Uninstall program

The Avaya IC 7.3.2 installation program installs an uninstall program that can uninstall the files from the IC 7.3.2 installation and returns your system to its previous state. If the installation fails, you must run the uninstall program before attempting to rerun the Installation program. Running the uninstall program preserves the files.

When the FP installer fails to complete the installation, any one of the following events might occur based on the progress achieved during installation:

- The uninstaller is created:

  You need to run the uninstaller to remove the FP to restore the system to its original state.

- The uninstaller is not created:

  When the uninstaller is not created, it implies that the FP installer has already rolled back all the changes made to the system during installation. In this case, no action is required from the user.

Before running the Uninstall program

Before uninstalling IC 7.3.2 FP, ensure that no instance of IC Java or Tomcat is running.

1. For uninstalling servers, stop all of the 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 directory to $AVAYA_IC73_HOME/lib.
- At the command line, type the following command: *slibclean*
- At the command line, 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 line:
  - 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 to restart the AIX machine.

Uninstalling IC 7.3.2

Perform the following steps on a system from where you want to uninstall IC 7.3.2 files:

1. Navigate to the following directory:

Windows: ...\IC73\ICServicePacks\7.3.2\<FolderNameOfComponent>\Record\

Solaris and AIX: .../IC73/ICServicePacks/7.3.2/<FolderNameOfComponent>/Record/

1. Start the Uninstall program:

Windows

- Double-click the uninstall7.3.2.bat file.

Solaris and AIX (server only)

1. At the command prompt, type: **`./uninstall7.3.2.sh`**.
2. Press **Enter**.
3. On the Welcome screen, click **Next**.
4. The next screen indicates the directory 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 machine for the system to be restored to its previous state. Solaris and AIX systems do not require restarting the machine.

Note: After the un-installation is complete, sometimes the uninstall program does not delete the 7.3.x, where 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.

Un-Installation using the Silent command line option

The IC 7.3.2 Service Pack components can be uninstalled using the Silent command line option. When you run un-installation in silent mode, the user interface is not available.

Silent mode

In a silent mode, rerun the same uninstallation in silent mode on another machine using the inputs from this text file.

To re-run the uninstaller in silent mode:

1. From the command prompt, go to the following directory:

   Windows:

   ...\IC73\ICServicePacks\7.3.2\<FolderNameOfComponent>\Record where <FolderNameOfComponent> is the folder name of each component where the respective component files reside.

   Solaris and AIX:

.../IC73/ICServicePacks/7.3.2/<FolderNameOfComponent>/Record where <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,

For example:

Operating System	Command
Windows	**uninstall7.3.2.bat -silent**
Solaris and AIX	**./uninstall7.3.2.sh –silent**

3. Press **Enter**.

Note: After the un-installation is complete, sometimes the uninstall program does not delete the 7.3.x (where x is SP number for which uninstall program is executed.For example, 7.3.2 for SP 2) subfolder or some of the sub-folders in it. In such a case, you need to manually delete the 7.3.x subfolder from the .../IC73/ICServicePacks folder.

Updating IC help

The IC help in HTML format is integrated with the IC application. When you install IC on a system, the installer updates the help files only for Avaya Agent and Avaya Agent Web Client components. For other IC components, the installer provides the `help.zip` file containing the required HTML help files. You need to manually extract these help files on the respective IC systems.

Note: In addition to the `help.zip` file available in the IC installer package, you can also download the latest `help.zip` file from 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 about updating the help by downloading the help.zip, see Updating the IC help by downloading the help.zip from the Avaya support site.

This section provides the procedures to update the help files for various IC components installed on Windows, Solaris, and AIX platforms.

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, and AIX system you need to 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.

- **IC732WinServer.zip**

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

  - Business advocate
  - Templatemanager
  - Webservices

- **IC732WinAdmin.zip**

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

  - Config accelerator (CA)
  - Database designer
  - IC Manager

- Report Wizard
- Workflowdesigner

- **IC732SolServer.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 installed IC Admin components, go to the `IC_INSTALL_HOME\IC73\help` directory.
2. (Optional) Backup all the files and folders from the help directory.
3. (Optional) From the IC installer, extract the **IC732WinAdmin** package.
4. From the extracted `IC732Admin` folder, open the `help.zip` file.
5. From the `help.zip` file, extract the `help` folder to the `IC_INSTALL_HOME\IC73\` directory 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 installed IC server components, go to the `IC_INSTALL_HOME\IC73\help` directory.
2. (Optional) Backup all the files and folders from the help directory.
3. (Optional) From the IC installer, extract the **IC732WinServer** package.
4. From the extracted `IC732WinServer` folder, open the help.zip file.
5. From the `help.zip` file, extract `help` folder to the `IC_INSTALL_HOME\IC73\` directory.

Installed on Solaris platform:

1. On the Solaris server where you installed IC server components, go to the `IC_INSTALL_HOME\IC73\help` directory.

2. (Optional) Backup all the files and folders from the help directory.
3. (Optional) From the IC installer, extract the **IC732SolServer** package.
4. From the extracted `IC732SolServer` 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` directory.

Installed on AIX platform:

1. On the AIX server where you installed IC server components, go to the `IC_INSTALL_HOME\IC73\help` directory.
2. (Optional) Backup all the files and folders from the help directory.
3. (Optional) 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` directory.

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	`IC_INSTALL_HOME\IC73\help`	Templatemanager webservices.html

	AIX	IC_INSTALL_HOME\IC73\help	Templatemanager webservices.html

Technical Support

If you experience trouble with IC 7.3.2, 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 its 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/.

Feature Pack files list

For information on the time stamp and version number of various service pack files for Avaya Interaction Center 7.3.x, see the *Service Pack file list with modification time stamp and version numbers for Avaya Interaction Center 7.3.x* document on the Avaya Support site: http://support.avaya.com/.

Customer found defects, known issues and workarounds, troubleshooting, and improvements

For information on issues and improvements included in Avaya Interaction Center 7.3.2 release, see the *List of Fixed Issues, Improvements, Known Issues and Workarounds, and Troubleshooting for Avaya Interaction Center 7.3.2* document on the Avaya Support site: http://support.avaya.com/

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 by telephone, call at one of the following numbers:

- Global Support Services (GSS) +1 800 242 2121
- Canada Customer Care Center +1 800 387 4268
- Remote Service Center Hungary +36 1238 8807
- Caribbean and Latin America +1 786 331 0860
- EMEA Services - Post Sales Technical Support +31 70 414 8720
- Asia/Pacific Regional Support Center +800 2 28292 78 / +65 6872 5141 and
- +0080066501243 (India)

For details on contact information, visit http://support.avaya.com/