Avaya Interaction Center

Installation and Configuration on Microsoft Windows/Oracle Solaris/IBM AIX

Release 7.3.x
Issue 7
November 2022

© 2022 Avaya Inc

All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN Avaya HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, http://support.avaya.com/LicenseInfo under the link "Avaya Terms of Use for Hosted Services" or such successor site as designated by Avaya, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in Section M(i)1 or 2 as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

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

Contents

Chapter 1: Introduction 18
Purpose 18
Intended audience 18
Document changes since last issue 18
Related resources 19
Documentation 19
Training 19
Viewing Avaya Mentor videos 20
Support 20

Chapter 2: Overview 22
Prerequisite skills and knowledge for installing InteractionCenter 22
IC installation files 23
Installing IC with Avaya Operational Analyst 24
Installation order 24
Installing IC with Avaya Operational Analyst 24
Database properties 25
Customizing Avaya IC 26

Chapter 3: Installing IC components 28
Before you install IC 29
Readme files 29
IC prerequisites 29
License file 29
Required administrator privileges 29
Hosting servers on Solaris 31
Hosting servers on AIX 31
Enabling short names on Microsoft Windows 32
Disable Java automatic downloading and updating 32
Caution and tips for installing IC components 32
Cautions and tips for installing IC servers 33
Cautions and tips for Design and Administration Tools 34
Installing IC server components 36
Configuring/workaround for Microsoft Windows 2019 support on IC 7.3.11 36
Configuring/workaround for Microsoft Windows 2012 R2 supporton IC 7.3.3 37
Configuration/workaround for Microsoft Windows 8.1 support onIC 7.3.3 37
Configuration/workaround for Microsoft Windows 10 support onIC 7.3.4 and later 38
Installing IC server and administration components on WindowsServer 2008 R2 or on Windows Server 2012 R2 39
Installing IC components on Solaris 41
Installing IC components on AIX 43

IC single box solution installation 45
IC single box solution components 45
IC single box solution client requirements 44
Configuring the ORB server environment 44
Configuring the primary ORB server environment 45
Configuring a secondary ORB server environment 47
Changing the ownership for IC 49
Changing ownership of the IC directories and files 50
Changing ownership only for Telephony server with Avaya switch 50
Setting up Business Advocate 51
Required administrator privileges for Business Advocate 51
Prerequisites for Business Advocate 52
Sharing the nethome directory 52
Configuring a Business Advocate environment 53
Building the database schema for the first Logical ResourceManager 54
Building the database schema for an additional Logical ResourceManager 58
Verifying permissions for running OA ECB with BusinessAdvocate 61
Installing Advocate Component Manager on a separate system 61
Installing the IC server SDK 63
Upgrading IC 64
Reinstalling IC components 64
Upgrading Daylight Saving Time (DST) patches 65

Chapter 4: Silent Install Interaction Center7.3 66
Option 1: Run the installer with default values (noresponse file) 66
Option 2: Using a response file to supply values forinstaller variables 67

Chapter 5: Configuring core servers 72
Before you configure IC core servers 72
Creating sites 73
Using IC domains 73
Preconfigured domains 74
Guidelines for IC domains 75
Creating domains 76
Establishing the failover order for domains 76
Setting up administrative accounts 77
About IC passwords 78
Using administrative accounts for non-human users 78
Using administrative accounts for human users 80
Creating administrative accounts 80
Using system and sample workflows 82
Sample workflows 82
Using sample workflows 83

Workflows in IC seed data 83
Configuring core servers 83
Server naming guidelines 84
Recommended tuning parameters for IC servers 85
Creating an ADU server 85
Creating a DUStore server 86
Creating a Directory server 88
Creating an EDU server 91
Creating a Report server 93
Creating a Workflow server 94
Creating a Blender server 98
Creating an HTTP Connector server 100
Creating a Notification server 103
Starting and stopping IC servers 107
Determining server dependencies 107
Starting and stopping the ORB server 110
Starting and stopping servers in IC Manager 112
Stopping all servers 112
Starting and stopping servers with the IC Admin utility 112
Starting and stopping IC services 114
Starting and stopping services on Windows 114
Starting and stopping services on Solaris 115
Starting and stopping services on AIX 118

Chapter 6: Configuring databases 122
Before you configure IC databases 122
Copying the stored procedure library - DB2 only 123
Setting up a Data server 123
Cautions and tips for configuring a Data server 124
Creating the primary Data server 124
Creating a secondary Data server 132
IC data sources 132
About data sources 132
Setting the display time for IC databases 133
Creating IC Repository 134
Before you create IC Repository 134
Building the IC Repository database 135
Generating the IC Repository application 142
Updating the Directory server with IC Repository 142
Creating the CCQ database 143
Modifying the Avaya Agent layout 144
Building the CCQ database 144
Generating the Interaction Center application 151

Chapter 7: Installing IC licenses 154
Before you configure IC licenses 154
Configuring the Web License Manager 155
Hosting multiple Web applications on one system 155
Advanced properties for the Web LM 156
Viewing license pick usage 156
Configuring the WebLM on Windows 156
Configuring the WebLM on Solaris 159
Configuring the WebLM on AIX 162
Installing the license file 165
Configuring the License server 167
Changing the administrative password 168
Managing users 169
Viewing server properties 170
Viewing information about configured licenses 170

Chapter 8: Configuring Telephony 172
Before you configure Telephony 173
Configuring the ACD name parameter 173
Creating the Telephony server 174
Configuring the Telephony server for Avaya CommunicationManager 175
Configuring Telephony Server for SIP 176
Creating a voice queue 178
Creating the Telephony Queue Statistics server 183
Configuring the TSQS server for Avaya Communication Manager 184
Starting the Telephony servers 185
Configuring a Workflow server for Telephony 186
Creating a Workflow server for Telephony 186
Configuring the voice channel for the Workflow server 187
Building and loading workflow for Telephony 189
Building the Incoming Call workflow 190
Loading workflows in the Workflow server 190
Creating routing hints for the Incoming Call workflow 191

Chapter 9: Configuring Web Management 194
Web Management support for media channels 195
Before you configure Web Management 195
Configuring servers for Web Management 196
Creating the WebACD server 196
Creating the Attribute server 200
Creating the ComHub server 202
Creating the Paging server 204

Starting the Web Management servers 206
Configuring Web Management services 206
Where to configure Web Management services 207
Hosting multiple Web applications on a system 207
Setting memory allocation for Web Management services 207
Configuring Web Management services on Windows 208
Configuring Internet Information Services 213
Configuring the Tomcat Redirector for IIS 215
Configuring Web Management services on Solaris 216
Configuring Web Management services on AIX 222
Integrating Web Management Administration 226
Integrating Web Management Administration with IC Manager 227
Setting the ServerName property - AIX only 228
Configuring a Workflow server for Web Management 229
Creating a Workflow server for Web Management 229
Creating the chat channel for the Workflow server 230
Using workflows for Web Management 232
Workflows required by Web Management 232
Reloading the customer management workflows 233
Configuring routing hints for the Qualify Chat workflow 234
Creating routing hints 234
Associating routing hints with Web Self-Service documents 236
Configuring the ICM server 237
Configuring IIS server for ICM support 239
Configuring the Central Internet Routing service 240
Configuring the Website 241
Configuring the IIS server on a separate system 244
Deploying Public website pages using ConfigIIS.bat tool 246
About ConfigIIS.bat tool 246
Configuring Avaya Full Text Search Engine 248
Configuring Avaya FTSE for Windows 248
Configuring for Avaya FTSE for Oracle Solaris 250
Configuring for Avaya FTSE for IBM AIX 253
Configuring Web Scheduled Callback 257
Cautions and tips for configuring Web Scheduled Callback 257
Creating a Web Scheduled Callback server 258
Configuring the Website for Web Scheduled Callback 259
Configuring Agents for Web Schedule Callback 260
Configuring Voice Chat 262
Prerequisites for Voice Chat 263
VoIP Configuration 263
Configure the Workflow server for Voice Chat 267

Build and load workflows for Voice Chat 270
Configure the Telephony server for Voice Chat 271
Configure the Voice Chat gateway 272
Configure the Voice Media Manager server 273
Configure the Voice Chat workflow table 274
Set the startup options for the VMM server 275
Configuring IC System for Voice Chat 276
Setting up a separate administration Website (optional) 277
Creating the Web application for the administration website 277
Configuring an administration Website 277
Integrating the administration Website 278
Setting up a separate customer Website (optional) 279
Creating the Web application for the customer Website 279
Configuring the customer Website 279
Deploying multiple ICM servers (optional) 280
Deployment guidelines for an additional ICM server 281
Before you configure an additional ICM server 281
Configuring an additional ICM server with a CIRS server 282
Configuring an independent additional ICM server 285
Adding ICM servers to the ICM Bridge 286
Refreshing IC Manager 286
Security configuration 287
Configuring the required security settings for your website 287

Chapter 10: Deploying CSPortal WebAPI 290
CSPortal WebAPI server side deployment 290
(Optional) Adding CSPortal configuration in IC Manager 291
Estimated Wait Time for Chat 293
Security configuration for CSPortal WebAPI Server 294
CSPortal WebAPI client side deployment 295
Deploying CSPortal WebAPI Client on Apache HTTP/HTTPS 296
Deploying CSPortal WebAPI Client on Microsoft IIS 297
Removing DWSensor plugin from IIS 300
Security configuration for CSPortal WebAPI Client 300
Uninstalling CSPortal 301

Chapter 11: Configuring IC Websites overHTTPS 304
Before you configure SSL 304
Configuring SSL on Windows 304
Reconfiguring website using the IC configure tool 305
Generating an IIS self-signed certificate 305
Binding the self-signed certificate 306
Adding the self-signed certificate to Trusted Root CertificateAuthorities 306

Editing webadmin configuration file 307
Modifying the website configuration 307
Configuring the WebACD server 308
Modifying the SSL properties 308
Exporting the CA certificate 309
About importing the CA certificate 309
Importing CA certificate in the Windows MMC console 310
Importing the CA certificate in the JAVA Keystore on servermachine where IC Manager is configured 311
Importing the CA certificate in the JAVA Keystore on server machine where Website and ICM are configured for SSL SMTP 312
Starting the IC Website, ICM, and Attribute Servers 313
Configuring SSL on Solaris 313
Reconfiguring the website using IC configure tool 313
Creating and installing the self-signed certificate in iPlanet 314
About exporting and importing a server self-signed certificate 316
Editing the configuration file 317
Modifying the website configuration 318
Configuring the WebACD server 318
Modifying the Group SSL properties 319
Configuring SSL on AIX 319
Reconfiguring Website using IC configure tool 319
Creating and configuring Self-Signed Certificate in IHS 320
Configuring the IHS httpd.conf file 321
Starting the IC Website, ICM and Attribute Servers 325

Chapter 12: Configuring Email Management 326
Before you configure Email Management 327
Configuring an IC Poller Server 327
Guidelines for IC Poller Server 327
Creating the IC Poller Server 327
Configuring an IC Email server 329
Guidelines for an IC Email server 329
Creating the IC Email server 329
Configuring Email Template Administration 333
Where to configure Email Template Administration 333
Hosting multiple Web applications on a system 333
Advanced properties for Email Template Administration 334
Configuring Email Template Administration on Windows 334
Configuring Email Template Administration on Solaris 336
Configuring Email Template Administration on AIX 339
Setting the options in Internet Explorer 341
Configuring a Workflow server for Email Management 342
Creating a Workflow server for Email Management 342

Creating email channels for the Workflow server 343
Starting the Workflow server 348
Using workflows for Email Management 348
Configuring Outbound Email Analysis workflows 348
Creating routing hints for email workflows 350
Configuring the WebACD server for Email Management 352
Integrating Email Template Administration 353
Configuring email accounts 354
Configuring the email accounts for SSL 364
Creating an email status 368
Configuring Avaya Content Analyzer (optional) 368
Creating the Administrative Content Analyzer server 369
Creating the Operations Content Analyzer server 370
Adding a Knowledge Base 372

Chapter 13: Configuring agent accounts 374
Required permissions for agents 375
Cautions and tips for creating agent accounts 376
Agent domains 376
Agent workgroups and tenants 376
Agent login IDs 377
Agent password requirements 377
Creating an agent account 378
Creating an agent account 378
Configuring an agent for media channels 382
Setting agent properties 384
Setting global properties for all agents 385
Setting properties for individual agents and workgroups 385
Configuring agents for Avaya Agent 386
Setting agent properties for Avaya Agent 387
Configuring agents for the Unified Agent Directory 388
Configuring agents for Avaya Agent Web Client 390
Configuring the working directory property 390
Configuring agents for the Address Book 391
Creating agents for a Client SDK custom application 392
Configuring the working directory property 392
Configuring agents for the Address Book 394
Configuring a Workflow server for transfers andconferences 395
Required configuration parameters 395
Working with transfer workflows 396
Configuring a Workflow server 396

Chapter 14: Deploying Avaya Agent 398

Required privileges for the agent installer ... 398
Creating installation files for agent applications ... 398
Cautions and tips for installation files ... 399
Required information for the Agent Site Preparation wizard ... 401
Running the Avaya Agent site preparation wizard ... 402
Copying the server implementation file ... 403
Preparing for installation by agents ... 404
Testing the agent installer ... 404
Creating installation instructions for agents ... 405
Configuring automatic updates for agent applications ... 406
Configuring WebAgent ... 408
Locating Application.properties file ... 409
Configuring the location to write the webagent logs ... 409
HTML Editor configuration for Rich Client ... 410
Configuring Avaya Agent to convert an email message to anattachment ... 412
Configuring auto flush ... 412
Configuring number of attachments to be displayed withoutscrollbar ... 412
Configuring the default location for saving attachment ... 413
Configuring default sorting ... 414
Configuring UTF-8 Encoding ... 414
Configuring Avaya Agent to populate Email templates ... 414
WebAgent HTML Editor ... 415
Hyperlink settings in Configuration XML ... 416
Configuring Hyperlink dialog box for HTML Email ... 418
Configuring the Citrix integration ... 419
About the Citrix integration ... 419
Installing the agent applications on the Citrix server ... 420
Deploying Citrix Xenapp 7.5 ... 420
Installing Citrix XenApp 7.5 ... 421
Configuring the XenApp 7.5 Site ... 423
Configuring the Virtual Delivery Agent software ... 424
Creating machine catalog ... 426
Configuring the Delivery group ... 427
Displaying or modifying the application properties ... 428
Deploying Avaya Agent Rich Client on the Citrix server ... 429
Locating the files for the tools ... 431
Citrix XenDesktop ... 431
Configuring the Avaya Agent INI file ... 432
Configuring the Web Client URL pre-requisite on CitrixXenDesktop Master Image ... 432
Configuring the IC Web browser tool ... 433
Configuring the executable tool ... 436
Sequence for using the Avaya tools for Citrix ... 440
Creating ICA (Citrix Client) connection with Citrix server ... 441

Chapter 15: Installing Avaya Agent Web 444
Prerequisites for Avaya Agent Web Client 445
IC components 445
Agent workstations 445
JRE version 446
Required administrator privileges 446
Working directory property 447
Internet connectivity 447
Installing the Avaya Agent Web Client 447
Creating the application WAR file 449
Setting up the Java Application Bridge 449
Configuring an agent account for the Java Application Bridge 449
Creating a Java Application Bridge 451
Setting up UNC to UNIX mapping 454
Installing the Avaya Agent Web Client Connector 456
Re-installing Avaya Agent Web Client connector 458

Chapter 16: Configuring and Deploying 460
Before you configure and deploy Avaya Agent Web Client 460
Configuring Avaya Agent Web Client 460
Basic Configuration 461
Running the configuration tool 461
Changing ownership for Avaya Agent Web Client on Solaris only 463
Changing ownership for Avaya Agent Web Client on AIX only 463
Starting and stopping Avaya Agent Web Client 463
Setting the options in Internet Explorer 9.0 and later 464
Testing Avaya Agent Web Client 466
Advance Configuration 466
Configuring SSL security for Avaya Agent Web Client (optional) 466
Verifying the deployment of AAWC 468
Redeploying the application WAR file 468

Chapter 17: Deploying Client SDK 470
Before you deploy Client SDK components 470
Installing the Client SDK components 471
Configuring a secondary ORB server environment 472
Client SDK files 472
Setting up the Java Application Bridge 473
Creating an agent account for the Java Application Bridge 473
Creating a Java Application Bridge 474
Configuring Client SDK services 476
Starting and stopping the Client SDK server 477

Starting and stopping the Client SDK server on Windows 477
Starting and stopping the Client SDK server on Solaris 478
Starting and stopping the Client SDK server on AIX 478
Enabling the SDK server for SSL (optional) 478
Configuring SDK Server with SSL on Java and Dotnet platform 479
Running a sample client 480
Optional advanced configuration for the Client SDK server 482
Configuring the log4j files for the Client SDK server (optional) 482
Changing default port range (optional) 483

Chapter 18: Deploying Web Services 484
Before you deploy Web Services components 484
Installing the Web Services components 485
Configuring a secondary ORB server environment 485
Web Services files 485
Setting up the Web Services Bridge 485
Creating an agent account for the Web Services Bridge 486
Creating a Web Services Bridge 487
Configuring Web Services 490
Starting and stopping the Web Services server 491
Starting and stopping the Web Services server on Windows 491
Starting and stopping the Web Services server on Solaris 491
Starting and stopping the Web Services server on AIX 492
Enabling the Web Services server for SSL 492
Removing IC Web Services 493

Chapter 19: Uninstalling IC 496
Uninstalling IC 496
Uninstalling IC components on Windows 496
Uninstalling IC servers on Solaris 497
Uninstalling IC servers on AIX 498
Uninstalling Web server components 498
Uninstalling related third-party components 499
Uninstalling Avaya Agent 499
Uninstalling Avaya Agent Web Client 500

Appendix A: Configuring a localized 502
About localized versions of IC 503
About the NLS Lang setting for Oracle 503
About the NLS Lang property 504
Where Oracle specifies the NLS Lang property 504
Cautions for the NLS Lang property 504
NLS Lang settings for supported languages 504

Enabling Database Designer for localization 505
Configuring Avaya Agent for a supported language 507
Configuring IC for multiple languages 508
Importing localized seed data 509
Configuring the website for supported languages 509
Setting language properties for agents 510
Localizing string table messages 512
Translating string table messages 512
Deleting string table messages 512
Configuring a Notification server for alternate emailencodings 513
Configuring an HTTP Connector server for TraditionalChinese 514
Configuring an HTTP Connector server for Russian 514
Configuring the Customer HTML Chat Client for JapaneseIMEs (optional) 515

Appendix B: Changing default service ports 516
Changing default service ports 516
Changing default ICM service ports 516
Changing default service ports for servers 518

Appendix C: Configuration Tool advanced 520
Accessing the advanced properties 520
Format of the advanced properties 521
Advanced properties 522
Using the recommended settings for the advancedproperties 523

Index 524

Chapter 1: Introduction

Purpose

The purpose of this guide is to provide detailed information about how to install and configure an out-of-the-box Avaya Interaction Center Release 7.3.x.

Intended audience

This guide is intended for those who use Avaya Interaction Center (IC). You should use this guide as an information source for:

- Installing all IC components.
- Configuring an out-of-the-box IC system for a development environment, without customizing.

Document changes since last issue

The following sections have been added or modified in this document since the last issue:

- Configuring SSL security for Avaya Agent Web Client
- Configuring the home directory property
- Configuring the location to write the webagent logs
- Configuring Avaya Agent to populate Email templates
- Internet Connectivity
- CSPortal WebAPI server side deployment

Related resources

Documentation

See the following related documents at http://support.avaya.com.

Title	Use this document to:	Audience
Avaya IC for Siebel Integration	get information about integration of Avaya IC for Siebel 8.1.1.x, 8.2.2.4, and 15	Supervisors Administrators Business Partners Administrators

Finding documents on the Avaya Support website

Use this procedure to find product documentation on the Avaya Support website.

1. Use a browser to navigate to the Avaya Support website at http://support.avaya.com.
2. At the top of the screen, enter your username and password and click **Login**.
3. Click **Documents**.
4. In the **Enter your Product Here** search box, type the product name and then select the product from the drop-down list.
5. If there is more than one release, select the appropriate release number from the **Choose Release** drop-down list.
6. Use the **Content Type** filter on the left to select the type of document you are looking for, or click Select All to see a list of all available documents.

   For example, if you are looking for user guides, select **User Guides** in the **Content Type** filter. Only documents in the selected category will appear in the list of documents.
7. Click **Enter**.

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. In the **Search** field, enter the course code, and click **Go to search** for the course.

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

Viewing Avaya Mentor videos

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

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

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In Search, type Avaya Mentor Videos to see a list of the available videos.
  - In Search, type the product name. On the Search Results page, select Video in the Content Type column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

Note:
Videos are not available for all products.

Support

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

Chapter 2: Overview

Avaya Interaction Center (Avaya IC) 7.3, a multi-channel contact center product, provides the latest platform support in the installation wizards. Avaya Interaction Center 7.3 ensures faster configuration using Configuration Accelerator.

The Avaya IC installation and configuration guide provides information and procedures about how to install and configure an out-of-the-box IC system.

If your Avaya IC system includes any customizations, you must first install a development system. You must test your customization on the development system before you deploy your customization.

This section describes useful information that you should know before you install and configure an Avaya IC system.

This section includes the following topics:

- Prerequisite skills and knowledge for installing Interaction Center on page 22
- IC installation files on page 23
- Installing IC with Avaya Operational Analyst on page 24
- Customizing Avaya IC on page 26

Prerequisite skills and knowledge for installing Interaction Center

Before you install Interaction Center, you must have working knowledge about the following:

- Operating Systems
  - Microsoft Windows Server 2012 R2 or Microsoft Windows Server 2008 R2
  - Oracle Solaris Release 10
  - AIX Release 6.1

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

  - Microsoft SQL Server
  - Oracle Database
  - IBM DB2
- Basic networking knowledge such as IP addressing, Firewall, and port configuration
- Web Server
  - Microsoft Internet Information Server (IIS)
  - Tomcat
  - Oracle iPlanet

IC installation files

The application and documentation files for Avaya Interaction Center 7.3 are available on http//www.avaya.com/support.

You can install Avaya Interaction Center on Windows, Solaris, and AIX operating system.

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

However, Avaya IC supports the following components only on Windows operating system:

- Business Advocate
- IC Manager
- Avaya Agent Rich Client
- Avaya Agent Web Client

Therefore, if you are installing Avaya IC on Solaris or AIX operating system, you must install the above components on Windows system and then integrate these components with the IC components that you install on Solaris or AIX operating system.

For more information about installing and configuring these components on Windows operating system, see the following guides:

- *Avaya IC Installation Planning and Prerequisites*
- *IC Business Advocate Configuration and Administration*
- *Avaya Agent User Guide*
- *Avaya Agent Web Client User Guide*

- *Avaya Agent Integration*

Installing IC with Avaya Operational Analyst

Avaya Operational Analyst (OA) provides reporting functionality for IC.

This section includes the following topics:

- Installation order on page 24
- Database properties on page 25

Installation order

You must follow the correct installation order to ensure that IC Repository is correctly configured for both IC and OA.

Install and configure the components of IC and OA in the following order:

1. Install and configure all prerequisites in the following documentation, including the installation of your database software and the creation of your database instance:
   a. For IC, see *Avaya IC Installation Planning and Prerequisites*.
   b. For OA, see *Operational Analyst Installation Planning and Prerequisites*.
2. Install the IC servers and administration components, as described in Installing IC server components on page 35.
3. Configure the additional IC components required for the deployment, as described in this manual.
4. Install and configure OA for IC, as described in *Operational Analyst Installation and Configuration*.

Installing IC with Avaya Operational Analyst

Avaya Operational Analyst (OA) provides reporting functionality for IC.

This section includes the following topics:

- Installation order on page 24
- Database properties on page 25

Database properties

Both Avaya IC and OA require access to the IC Repository database.

Avaya IC and OA use the values given in the following table for their database properties:

Property	DB2	Oracle	SQL Server
Database Administration Login	db2inst1	System	sa level user name
Database Administration Password	db2inst1 password	system password	sa level password
IC Repository database name See Configuring the IC Repository database connection on page 135.	Database schema name that you enter in Database Designer. For example, **repository**.	Database name for the Oracle user that you enter in Database Designer. For example, **repository**.	Database name that you enter in Database Designer. For example, **repository**.

Property	DB2
Database Administration Login	db2inst1
Database Administration Password	db2inst1 password
IC Repository database name See Configuring the IC Repository database connection on page 135.	Database schema name that you enter in Database Designer. For example, **repository**.

Property	Oracle
Database Administration Login	system
Database Administration Password	system password
IC Repository database name See Configuring the IC Repository database connection on page 135.	Database name for the Oracle user that you enter in Database Designer. For example, **repository**.

Customizing Avaya IC

If your Avaya IC system includes customizing requirements, use this guide to install a development system. Use the development system to test and, if required, customize your Avaya IC system.

For more information on how to customize the Avaya IC components, see the other documentation in the Avaya IC documentation set. The introduction provided on the Avaya IC documentation includes a complete description of all documentation in the Avaya IC documentation set.

The following table describes some of the IC documentation that you can use to customize an Avaya IC system:

IC Component	Documents
Avaya Agent	• *Avaya Agent Integration* • *Interaction Center Administration Guide*
Avaya Agent Web Client	• *Avaya Agent Web Client Customization* • *Interaction Center Administration Guide*
IC databases and data models	• *IC Database Designer Application Reference* • *Data Model files*
Client SDK	• *Avaya IC Client SDK Programmer Guide*
Servers	• *Interaction Center Administration Guide* • *Agent Data Unit Server Programmer Guide* • *Electronic Data Unit Server Programmer Guide* • *Avaya IC Telephony Connectors Programmer Guide* • *Core Services Programmer Guide* • *Avaya IC Client and Server Programmer Design Guide* • *Avaya IC Integration with VP / IR*
Telephony	• *Interaction Center Administration Guide* • *Avaya IC Telephony Connectors Programmer Guide* • *Avaya IC Integration with VP / IR* • *External Function Library for Avaya IVR* • *IC/OA Software Upgrade and Data Migration*
Web Services	• *Avaya IC Web Services Programmer Guide*

IC Component	Documents
Workflows	• *Avaya IC Workflow Designer User Guide* • *Avaya IC Workflow API Reference* • *Avaya IC Media Workflow Reference* • *Agent Script Workflow Reference* • *Avaya IC Scripts Language Reference* • *Avaya IC Scripts VBA Scripting Reference*
Avaya Business Advocate	• *IC Business Advocate Configuration and Administration* • *Avaya IC Media Workflow Reference*
IC for Siebel 8.1.1.x, 8.2.2.x, and 15	• *Avaya IC for Siebel Integration*

Chapter 3: Installing IC components

Install and configure the Avaya IC components in the order of topics appearing in this section. For example, install and configure the primary servers before you install and configure the Design and Administration Tools.

This section includes the following topics:

- Before you install IC on page 29
- Caution and tips for installing IC components on page 32
- Installing IC server components on page 35
- Configuring the ORB server environment on page 44
- Changing the ownership for IC on page 49
- Setting up Business Advocate on page 51
- Installing the IC server SDK on page 63
- Upgrading IC on page 64
- Reinstalling IC components on page 64
- Upgrading Daylight Saving Time (DST) patches on page 65

CAUTION:
Do not install IC on a system that also hosts the software that filters or controls network access. These software can cause IC to fail or impact performance. For example, website filters or software firewalls can affect network access in several ways. The website filters or software firewalls can cause a slowdown in network access, cause applications that open a large number of sockets to fail, or rewrite packets.

For information about deploying IC agent applications, see:

- Deploying Avaya Agent on page 398
- Installing Avaya Agent Web Client on page 444
- Deploying Client SDK components on page 470

Before you install IC

This section describes the steps that you must perform before you install IC components. This section includes the following topics:

- Readme files on page 29
- IC prerequisites on page 29
- License file on page 29
- Required administrator privileges on page 29
- Hosting servers on Solaris on page 31
- Hosting servers on AIX on page 31
- Disable Java automatic downloading and updating on page 32

Readme files

Read the IC Readme file on the CRM Technical Support website at http://www.avaya.com/support/.

IC prerequisites

Read the *Avaya IC Installation Planning and Prerequisites* and install all prerequisite components.

License file

Obtain the necessary IC license file for your IC system. For more information, see *Avaya IC Installation Planning and Prerequisites*.

Required administrator privileges

All IC users who perform certain tasks require administrator privileges. This section describes the administrator privileges required on the operating system:

- Required administrator privileges for Windows on page 30
- Required administrator privileges for Solaris on page 30

- Required administrator privileges for AIX on page 30

Required administrator privileges for Windows

All IC users who perform the following tasks must have a Windows Administrator login or a Windows login with administrator privileges:

- Install and configure IC servers
- Install or use Design and Administration Tools

Required administrator privileges for Solaris

All IC users, who install and configure IC servers, require one of the following UNIX accounts, depending upon which tasks the users need to perform.

Root user: You need this account when you:

- Install IC on a system that hosts a Telephony server for an Avaya switch with Communication Manager.
- Configure the Web applications with the Configuration Tool, including the website, Email Template Administration, and Web License Manager.

Installation user: You need this account to perform all the tasks to configure IC that does not require the root user. The IC installation directory must be owned by this account.

For example, you can create an installation user account named **avaya**.

Important:
If you do not use a root account to install Avaya IC servers on a system, and need to configure that system with a Telephony server for an Avaya switch with Communication Manager software, reinstall the Avaya IC servers using the root account.

Required administrator privileges for AIX

All IC users, who install and configure IC servers, require one of the following UNIX accounts, depending upon which tasks they need to perform:

Root user: You need this account when you:

- Install IC on a system that will host a Telephony server for an Avaya switch with Communication Manager.
- Configure the Web applications with the Configuration Tool, including the website, Email Template Administration, and Web License Manager.

Installation user: You need this account to perform all the tasks to configure IC that does not require the root user. This account must own the IC installation directory.

For example, you can create an installation user account named **avaya**.

Important:
If you do not use a root account to install Avaya IC servers on a system, and need to configure that system with a Telephony server for an Avaya switch with Communication Manager software, reinstall the Avaya IC servers using the root account.

Hosting servers on Solaris

If you host your servers on Solaris:

- Install a Windowing environment, such as X-Windows.
- Set the `DISPLAY` parameter.
- Ensure that the server has enough space in the `/var/tmp` directory for installing Java Virtual Machine. The IC installer requires at least 2048-MB of extra temporary space.
- Install appropriate locales for languages supported by your system. For more information about the required locales, see *Avaya IC Installation Planning and Prerequisites*.

Hosting servers on AIX

If you host your servers on AIX:

- Install a Windowing environment, such as X-Windows.
- Set the `DISPLAY` parameter.
- Make sure that the server has enough space in the `/tmp` directory for installing Java Virtual Machine. The IC installer requires at least 2048-MB of extra temp space.
- Install appropriate locales for languages supported by your system. For more information about the required locales, see *Avaya IC Installation Planning and Prerequisites*.

Enabling short names on Microsoft Windows

Before you install IC 7.3.x, if AVAYA_IC73_HOME path is set to non-default path such as "C:\Program Files (x86)\Avaya\IC73" which is formed using either brackets or spaces or folder name consists more than 8 characters then ensure that short names (8.3 pattern) is enabled on Microsoft Windows operating system. For more information on short file names see the following article on the Microsoft website at https://support.microsoft.com/en-us/kb/121007

Note:

The default install path of Avaya Interaction Center on Microsoft Windows operating system is **`C:\Avaya\IC73`**

Disable Java automatic downloading and updating

All IC users who install and configure IC components are required to disable the automatic updating options for Java. Perform the following steps:

1. From the Windows Control Panel, run the **Java** program.

   The **Java Control Panel** window opens.
2. On the **Update** tab, clear the **Check for Updates Automatically** check box.
3. Click the **Advanced** tab.
4. Expand the **JRE Auto-Download** node.
5. Select the **Never Auto-Download** option.
6. Click **OK**.

Note:

For details on the supported version of Java JRE, refer to the *Avaya IC Installation Planning and Prerequisites* guide.

Caution and tips for installing IC components

This section includes the following topics:

- Cautions and tips for installing IC servers on page 33
- Cautions and tips for Design and Administration Tools on page 34

Cautions and tips for installing IC servers

Consider the following important cautions and tips when you install IC servers:

- Required disk space on page 33
- HP Openview on page 33
- Installation mode on page 34
- Cautions and tips for Design and Administration Tools on page 34

Required disk space

Ensure that you have sufficient disk space on the target system to install selected files. The IC installation does not check the free disk space available on your system until you select the components to install. For details on the required disk space for Avaya IC installation, refer to the *Avaya IC Installation Planning and Prerequisites* guide.

HP Openview

If you are installing ORB server on a system that already hosts HP Openview, you must turn off the HP Openview before installing ORB server. HP Openview may prevent the Avaya IC installer from copying all the required files to the *IC_INSTALL_DIR*\IC73\bin directory.

In the Windows environment, you can turn off HP Openview by stopping the `HP ITO Agent` service from the Windows Services control panel.

Tip:
You can open Windows Services control panel by running the **services.msc** command.

For more information about HP Openview, see the documentation provided by HP.

Installation mode

All Avaya IC installers can run in GUI, Console, and Silent mode. GUI is the default installation mode for all the installers.

Cautions and tips for Design and Administration Tools

Consider the following important cautions and tips when you install and use the IC Design and Administration Tools:

- Components installed with Design and Administration Tools on page 34
- Design and Administration systems on page 34
- Supported operating systems on page 34
- Running multiple instances of IC Manager on page 35

Components installed with Design and Administration Tools

IC installs all the Design and Administration Tools on the target system. You cannot select individual tools to install.

The tools and files that Avaya IC installs with the Design and Administration Tools are:

- IC Manager
- Avaya Workflow Designer with blocks, sample workflows, and related files
- Avaya Database Designer with the Avaya IC Script Editor, design files, and related files
- ICDoctor
- LogCollector
- Config Accelerator

Design and Administration systems

IC Manager and other administrative applications can potentially consume a significant amount of CPU resources. To ensure that the requirements of IC Manager do not interfere with the performance of your IC servers, deploy your Design and Administration Tools on a dedicated system.

Supported operating systems

Design and Administration Tools work only on a supported Windows operating system. For more information, see *Avaya IC Installation Planning and Prerequisites*.

Running multiple instances of IC Manager

IC Manager does not support concurrent administration. When an administrator selects and updates a record, such as a server or an agent, IC Manager does not lock that record. Any other administrator can open and update the same record.

CAUTION:
Simultaneous administration of servers, domains, and Directory server tables in more than one IC Manager can corrupt the configuration files and results in the loss of configuration data.

If you plan to have more than one instance of IC Manager, you must clearly define the administrative policies for IC. For example:

- Use only one instance of IC Manager at a time to administer servers.
- Determine which IC elements an administrator can update, and assign the appropriate permissions to the login ID for that administrator.
- Do not allow administrators to log in to more than one instance of IC Manager with the same login ID and password.

For more information about multiple instances of IC Manager, see *Interaction Center Administration Guide*.

Installing IC server components

Tip:
For information about the components on each IC CD/DVD-ROM, see IC installation files on page 23.

This section includes the following topics:

- Configuring/workaround for Microsoft Windows 2019 support on IC 7.3.11 on page 36
- Installing IC server and administration components on Windows Server 2008 R2 or on Windows Server 2012 R2 on page 37
- Installing IC components on Solaris on page 39
- Installing IC components on AIX on page 41

Configuring/workaround for Microsoft Windows 2019 support on IC 7.3.11

You need to do the following steps in case when you renamed icemailsrv.exe or pollersrv.exe

binaries.

Configuration for Core Server Installer:

1. Go to the system's **Settings**, **Updates & Security**, **Windows Security**, **App & browser control**, **Exploit protection settings**, **Program settings**.
2. Select **Add program to customize**, then an appropriate option between **Add by program name** and **Choose exact file path**.
3. Enter the name or full path then click **Add**.
4. In the **Program settings** panel scroll down to **Randomize memory allocations (Bottom-up ASLR)** and check the box then move slider to "On" position.
5. Click **Apply**.
6. Repeat 3-5 for all yours renamed binaries.

Configuring/workaround for Microsoft Windows 2012 R2 support on IC 7.3.3

Configuration for Core Server and Web Connector Installer:

7. Right-click the RTM installer and click **Properties**.
8. In the **Properties** window, go to **Compatibility** tab.
9. In the Compatibility mode section, select **Run this program in compatibility mode for** option, and from the drop-down menu, select **Windows 7**.
10. In the **Privilege Level** section, select **Run this program as an administrator** option.
11. Click **Apply**.

Configuration/workaround for Microsoft Windows 8.1 support on IC 7.3.3

Configuration for Design & Admin and Rich Client Installer:

1. Right-click the RTM installer and click **Properties**.
2. In the **Properties** window, go to **Compatibility** tab.
3. In the Compatibility mode section, select **Run this program in compatibility mode for** option, and from the drop-down menu, select **Windows 7**.
4. In the **Privilege Level** section, select **Run this program as an administrator** option.
5. Click **Apply**.

Configuration/workaround for Microsoft Windows 10 support on IC 7.3.4 and later

Configuration for Design & Admin and Rich Client Installer:

1. Right-click the RTM installer and click **Properties**.
2. In the **Properties** window, go to **Compatibility** tab.
3. In the Compatibility mode section, select **Run this program in compatibility mode for** option, and from the drop-down menu, select **Windows 7**.
4. In the **Privilege Level** section, select **Run this program as an administrator** option.
5. Click **Apply**

Installing IC server and administration components on Windows Server 2008 R2 or on Windows Server 2012 R2

You can install only one component at a time with the IC Windows Servers, Administration installer. You cannot select multiple components to install simultaneously.

To install IC server and administration components on Windows:

1. Log in to the system with an account that has the required Administrator privileges.
2. Download and install the setup file from the CD/DVD-ROM:
   a. Insert IC Release 7.3 CD/DVD-ROM 1.
   b. From the CD/DVD-ROM double click the `install.html` file.
   c. The Internet Explorer window opens the **Welcome** page and a button to download the installer.
   d. Click the **Download Installer for Windows** button.

      The **File Download** dialog box opens with options for running or saving the installer.
   e. Click **Run** to run the installer from the server.

      OR

      Click **Save** to first save the installer on your local system and then run it.
3. When the IC installer opens, read the entire IC license agreement carefully, and then accept the terms of the agreement. Select **Next** and then follow the prompts in the installer.

Note:
The IC installer exits if you do not agree to the terms of the agreement.

4. In the Choose Install Folder, click **Next**. The default installation folder is D:\Avaya if D drive exists, else the drive letter will be C:\Avaya.

Note:
You must use short folder names to ensure a successful startup. Long folder names such as, Program Files (x86) or folder names with special characters and spaces might cause path breaks and result in the Tomcat server not being able to start successfully.

5. In the **Product Installation** screen, select one of the options from the following table to install the required component:

Option	Installation location	Files Installed
Core Servers	Core server systems	• IC core servers • Avaya Full Text Search Engine • Web Scheduled Callback • Business Advocate servers and Administrative Client • Client SDK components • Web Services components • SDK Server • ConfigTools
Avaya IC Design and Administration Tools	Design and administration system	• IC Manager • Business Advocate Administrative Client • Database Designer • Workflow Designer • ICDoctor • LogCollector • Config Accelerator • ConfigTools
Avaya Agent Web Connector	Avaya Agent Web Connector system	• Vesp and DCO bridges • ConfigTools

Note:

The **Visual C++ Redistributable Installation** dialog box appears. Click **Yes** to install the Visual C++ runtime libraries. VCRedist is a Microsoft re-distributable package 'Visual C++ 2005 SP1 (MFC security update)' that installs Visual C++ runtime libraries required to run Avaya IC. If Visual C++ 2005 SP1 or a later is already installed by another application, you can skip this installation. Click **No** to skip VCRedist package installation.

6. Continue to follow the prompts in the IC installer.

   The IC installer can take several minutes to copy the requested files to the system. If the target system does not have sufficient space to install the components, the IC installer displays an error message.

7. The installer displays a message after installing Avaya IC successfully.

8. The next step in the IC installation depends upon the components you want to host on the target system. Perform one of the following steps:

Type of configuration	Location of steps
Primary ORB server system	Configuring the primary ORB server environment on page 45
Secondary ORB server system, including Client SDK server system	Configuring a secondary ORB server environment on page 47
Design & Administration	
Avaya Agent Web Client	Installing Avaya Agent Web Client on page 444

Note:
Verify that the AVAYA_IC73_HOME environment variable is correctly set to IC_INSTALL_DIR\IC73\.

Installing IC components on Solaris

CAUTION:
Do not install IC servers if you have not yet installed the appropriate locales for Solaris operating system. For more information about the required locales, see *Avaya IC Installation Planning and Prerequisites*.

Using the IC Solaris Servers installer, you can install only one component at a time. You cannot select multiple components to install simultaneously.

To install IC server components:

1. Log in to the system with an account with the required Administrator privileges.
2. Download the installer:
   a. Insert IC Release 7.3 CD/DVD-ROM 2.
   b. From the CD/DVD-ROM double click the `install.html` file.
   c. The browser window opens with **Welcome** page and a button to download the installer.
   d. Click the **Download Installer for Solaris SPARC** button for downloading the Solaris installer:
   e. The system displays the **File Download** dialog box with options for running or saving the installer.

f. Click **Run** to run the installer from the server.

OR

g. Click **Save** to first save the installer on your local system and then run it.

Tip:
If Avaya IC installer does not start automatically, follow the instructions given on the **Welcome** screen.

3. When the IC installer opens, read the entire IC license agreement carefully, and then accept the terms of the agreement. Click **Next** and then follow the prompts in the installer.

Note:
The IC installer exits if you do not agree to the terms of the agreement.

4. On the **Product Installation** screen, select one of the options from the following table to install the required component:

Option	Location	Files Installed
Core Servers	Core server system	• IC core servers • Avaya Full Text Search Engine • Web Scheduled Callback • Business Advocate Telephony Services Adaptor and Web Advocate Adaptor servers only • Client SDK components • Web Services components • SDK Server • ConfigTools
Avaya Agent Web Connector	Avaya Agent Web Connector system	• Vesp and DCO bridges • ConfigTools

5. Continue to follow the prompts in the IC installer.

   The IC installer can take several minutes to copy the requested files to the system. If the target system does not have sufficient space to install the components, the IC installer displays an error message.

6. The next step in the IC installation depends upon the components you want to host on the target system. Perform one of the following steps:

System	Steps
Primary ORB server system	Configuring the primary ORB server environment on page 45
Secondary ORB server system, including Client SDK server system	Configuring a secondary ORB server environment on page 47
Avaya Agent Web Client	Installing Avaya Agent Web Client on page 444

Note:

Verify that the AVAYA_IC73_HOME environment variable is correctly set to IC_INSTALL_DIR/IC73/. Set the environment variable if not already set.

Installing IC components on AIX

CAUTION:

Do not install IC servers on AIX if you have not yet installed the appropriate locales for AIX operating system. For more information about the required locales, see *Avaya IC Installation Planning and Prerequisites*.

You can install only one component at a time with the IC AIX Servers installer. You cannot select multiple components to install simultaneously.

Note:

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

To install IC server components on AIX:

1. Log in to the system with an account with the required Administrator privileges.
2. Download the ISO and burn the IC 7.3 CD/DVD for AIX:
   1. Insert IC Release 7.3 CD/DVD-ROM 3 for AIX servers.

2. From the CD/DVD-ROM double click the `install.html` file.

   The browser window opens the **Welcome** page and a button to download the installer.

3. Click the **Download Installer for AIX** button for downloading the AIX installer.

   The system displays the **File Download** dialog box with options for running or saving the installer.

4. Click **Run** to run the installer from the server.

   OR

5. Click **Save** to first save the installer on your local system and then run it.

Tip:
If Avaya IC installer does not start automatically, follow the instructions given on the **Welcome** screen.

3. When the IC installer opens, read the entire IC license agreement carefully, and then accept the terms of the agreement. Click **Next**, and then follow the prompts in the installer.

Note:
The IC installer exits if you do not agree to the terms of the agreement.

4. In the Product Installation screen, select one of the options in the following table to install the required component:

Option	Location	Files Installed
Core Servers	Core server system	• IC core servers • Avaya Full Text Search Engine • Web Scheduled Callback • Business Advocate Telephony Services Adaptor and Web Advocate Adaptor servers only • Client SDK components • Web Services components • SDK Server • ConfigTools
Avaya Agent Web Connector	Avaya Agent Web Connector system	• Vesp and DCO bridges • ConfigTools

5. Continue to follow the prompts in the IC installer.

   The IC installer can take several minutes to copy the requested files to the system. If the target system does not have sufficient space to install the components, the IC installer displays an error message.

6. The next step in the IC installation depends upon the components you want to host on the target system. Perform one of the following steps:

System	Steps
Primary ORB server system	Configuring the primary ORB server environment on page 45
Secondary ORB server system, including Client SDK server system	Configuring a secondary ORB server environment on page 47
Avaya Agent Web Client	Installing Avaya Agent Web Client on page 444

Note:

Verify that the `AVAYA_IC73_HOME` environment variable is correctly set to `IC_INSTALL_DIR/IC73/`. Set the environment variable if not already set.

IC single box solution installation

The procedures for installing and configuring IC components is a single box solution is the same as the procedures for Avaya Interaction Center 7.3.x across multiple machines.

IC single box solution components

The following components are part of the IC single box solution:

- IC Servers
- Either IC CSPortal Service OR IC website
- IC SDK Service
- IC ICM Service
- IC Template Administration
- AOA Server
- IC BA (Only Primary LRM)

- HTTPVox
- IC WebLM Service

See Avaya Interaction Center and Avaya Operational Analyst Overview and Specification for information on configuring IC tunable parameters.

The following components are not part of the IC single box solution:

- IC Web Connector
- ICEmail / Poller and WACD cluster failover
- IC website if CSPortal is hosted on a Single box primary ORB
- Additional LRM

You can host the following components on a separate secondary ORB server for redundancy:

- ICEmail / Poller and WACD cluster failover
- TS Multi-Site Heterogeneous Switch (MSHS)
- IC website if CSPortal is hosted on a Single box primary ORB
- Additional LRM

IC single box solution client requirements

You require client machines for the following components:

- Design and Admin
- OA Admin Client
- Rich Client
- CSPortal client (MS-IIS / Apache web server)

Configuring the ORB server environment

Important:
For Solaris and AIX, the Configuration Tool changes the ownership of the implementation file (vesp.imp) and the interface file (vespidl.pk) to root. If you do not want to run IC as root, you must change the ownership of these files. For more information, see Changing the ownership for IC on page 49.

You must run the Configuration Tool on every system that hosts an ORB server to create a server environment. The configuration mode that you select in the installer depends upon the type of ORB server that you plan to host on the system.

The system that hosts the primary ORB server requires a primary server environment. All other systems require a secondary server environment.

This section includes the following topics:

- Configuring the primary ORB server environment on page 45
- Configuring a secondary ORB server environment on page 47

Configuring the primary ORB server environment

This procedure is a continuation of Installing IC server components on page 35.

To configure the primary server environment:

1. In the Configuration Tool, click the **Initial Configuration** tab.
2. From the **Select Mode** drop-down list, select **Primary**.
3. Confirm that the IP address in the **IP Address** drop-down list is the correct IP address for the system that hosts the primary ORB server.

   Important:
   If the ORB server runs on a system with multiple network interface cards, you must select the IP address for the first network interface card on the system. The ORB server cannot run on any other network interface card.
4. Ensure the port assignment in the **Start Port** field is an available port on the target system. Type a new port assignment if necessary.
5. Click **Start ORB Server**.
6. If the system is hosting a Telephony server:
   a. Select and check the **Telephony Switch** box.
   b. From the **Telephony Switch** drop-down list, select the name of the switch with which the Telephony server will communicate.

      The Telephony server must communicate with a switch that is supported for the operating system of the system. For example, do not select a Nortel switch if you plan to host the Telephony server on an AIX system. For more information about switch support, see *Avaya IC Installation Planning and Prerequisites*.
7. If the IC system includes an Oracle database:
   a. Select and check the **Oracle Setup** box.

b. Type the NLS Lang parameter in the **NLS Lang** field to specify the character set of the database.

   The NLS Lang setting must match the value used to create the Oracle database. This value must include UTF8. For example, if your database uses US English language conventions, enter **`AMERICAN_AMERICA.UTF8`**. For more information, see About the NLS Lang setting for Oracle on page 503.

c. Type the home directory of the Oracle client on the system that hosts the core servers in the **Oracle Home** field.

   For example, type `C:\app\client\administrator\product\<oracle_version>\client_1`

d. For Oracle databases, type the Oracle SID of the database in the **Oracle SID** field.

   For example, type `icutf8db`. The Oracle SID field is case-sensitive.

e. For Oracle databases, select the correct version of Oracle Database server from the **Oracle Version** field.

8. If the IC system includes a DB2 database:

   a. Select the **DB2 Setup** box.

   b. Type the home directory of the DB2 client on the system that hosts the core servers in the **DB2 Home** field.

      For example, type `/usr/lpp/db2_ic`

   c. Type the name of the DB2 instance in the **DB2 Instance** field.

      For example, type `db2inst1`

9. If you host the servers on Solaris, select the primary locale from the **Locale** drop-down list.

   The drop-down list includes all of the locales supported by the operating system. For example, if your servers use an English locale, select en_US.UTF-8.

10. If you host the servers on AIX, select the primary locale from the **Locale** drop-down list.

    The drop-down list includes all of the locales supported by the operating system. For example, if your servers use an English locale, select en_US.

11. Click **Apply Settings** in the Configuration Tool to configure and start the core servers.

12. Click **OK**.

13. Click **Exit**.

    The Configuration Tool closes and returns you to the Avaya IC installer.

14. In the IC installer, follow the prompts.

    If you leave the **View Readme** field selected, the IC Readme opens in Adobe Acrobat. After you have reviewed the Readme, close Acrobat to return to the IC installer.

    The Readme is available on the CD/DVD-ROM.

The Readme is available on the CD/DVD-ROM.

15. The next step in the IC installation depends upon the components you want to host on the target system. Perform one of the following steps:

Type of servers	Location of steps
Core servers without Business Advocate	Configuring databases on page 122
Core servers with Business Advocate	Setting up Business Advocate on page 51
Client SDK server components	Deploying Client SDK components on page 470

Configuring a secondary ORB server environment

This procedure continues from Installing IC server components on page 35.

To configure the secondary server environment:

1. In the Configuration Tool, click the **Initial Configuration** tab.
2. From the **Select Mode** drop-down list, select **Secondary**.
3. Confirm that the IP address in the **IP Address** drop-down list is the correct IP address for the system that hosts the secondary ORB server.

   Important:
   If the secondary ORB server runs on a system with multiple network interface cards, you must select the IP address for the first network interface card on the system. The ORB server cannot run on any other network interface card.
4. Make sure the port assignment in the **Secondary ORB Port** field is an available port on the target system. Type a new port assignment if necessary.
5. In the **Primary Host Name** field, type the IP Address or the fully-qualified domain name of the system that hosts the primary ORB server.
6. In the **Primary ORB Port** field, confirm that the port is the same you configured for the primary ORB server.
7. In the **IC Login** field, type the administrative login ID that will run the Avaya IC servers.

   For more information, see Setting up administrative accounts on page 77.
8. In the **IC Password** field, type the password associated with the Avaya IC Login.
9. In the **IC Domain** field, type the name of the IC domain that includes the primary ORB server. This domain is typically the Default domain.
10. Select **Start ORB Server**.

11. If the system is hosting a Telephony server:
    a. Select and check the **Telephony Switch** box.
    b. From the **Telephony Switch** drop-down list, select the name of the switch with which the Telephony server will communicate.

       The Telephony server must communicate with a switch that is supported for the operating system of the system. For example, do not select a Nortel switch if you plan to host the Telephony server on an AIX system. For more information about switch support, see *Avaya IC Installation Planning and Prerequisites*.
12. If the IC system includes an Oracle database:
    a. Select and check the **Oracle Setup** box.
    b. Type the NLS Lang parameter in the **NLS Lang** field to specify the character set of the database.

       The NLS Lang setting must match the value used to create the Oracle database. This value must include UTF8. For example, if your database uses US English language conventions, enter **`AMERICAN_AMERICA.UTF8`**. For more information, see About the NLS Lang setting for Oracle on page 503.
    c. Type the home directory of the Oracle client on the system that hosts the core servers in the **Oracle Home** field.

       For example, type `/opt/oracle/Ora_ic`
    d. For Oracle databases only on Solaris, type the Oracle SID of the database in the **Oracle SID** field.

       For example, type `icutf8db`. The Oracle SID field is case-sensitive.
    e. For Oracle databases only on Solaris, select the correct version of Oracle from the **Oracle Version** field.
13. If the IC system includes a DB2 database:
    a. Select and check the **DB2 Setup** box.
    b. Type the home directory of the DB2 client on the system that hosts the core servers in the **DB2 Home** field.

       For example, type `/usr/lpp/db2_ic`
    c. Type the name of the DB2 instance in the **DB2 Instance** field.

       For example, type `db2inst1`
14. If you host the servers on Solaris, select the primary locale from the **Locale** drop-down list.

    The drop-down list includes all of the locales supported by the operating system. For example, if your servers use an English locale, select en_US.UTF-8.
15. If you host the servers on AIX, select the primary locale from the **Locale** drop-down list.

    The drop-down list includes all of the locales supported by the operating system. For example, if your servers use an English locale, select en_US.

16. Click **Apply Settings** in the Configuration Tool to configure and start the core servers.
17. Click **OK**.
18. Click **Exit**.

    The Configuration Tool closes and returns you to the Avaya IC installer.
19. In the IC installer, follow the prompts.

    If you leave the **View Readme** field checked, the IC Readme opens in Adobe Acrobat. After you have reviewed the Readme, close Acrobat to return to the IC installer.

    The Readme is available on the CD/DVD-ROM.
20. The next step in the IC installation depends upon the components you want to host on the target system. Perform one of the following steps:

Type of servers	Location of steps
Core servers without Business Advocate	Configuring databases on page 122
Core servers with Business Advocate	Setting up Business Advocate on page 51
Client SDK server components	Deploying Client SDK components on page 470

Changing the ownership for IC

If you installed IC as the root user and do not want to run IC servers and services as root on your system, you need to change the ownership of the Avaya IC directories and files.

Important:
For security reasons, users must avoid running IC software as the root user wherever possible. Create a user for the IC system before you perform these steps. For more information, see *Avaya IC Installation Planning and Prerequisites*.

This section includes the following steps that you must perform if you do not want to run IC as root:

1. Changing ownership of the IC directories and files on page 50
2. Changing ownership only for Telephony server with Avaya switch on page 50

Changing ownership of the IC directories and files

To change ownership of the IC directories and files:

1. Log in as root user.
2. Navigate to *IC_INSTALL_DIR*/IC73/bin.
3. Shutdown all IC servers. For more information, see Stopping all servers on page 112.
4. Navigate to the parent directory of *IC_INSTALL_DIR*/IC73/.
5. Execute the following command:

   chown -R <avayauser>:<avayagroup> IC73

   where <*avayauser*> represents the non-root user that you use to run the IC components and <*avayagroup*> is the primary group for <*avayauser*>.
6. Switch to <*avayauser*> and restart the IC servers. For more information, see Starting and stopping servers in IC Manager on page 112.

Changing ownership only for Telephony server with Avaya switch

For a system that includes an Avaya switch with Communication Manager, change the ownership of every Telephony server.

You configure the SUID bit and root ownership to ensure that the Telephony server for the Avaya switch can start up as the root user to enable agent event reporting. The Telephony server resets its process user ID to <*avayauser*> immediately after startup.

To change ownership for the Telephony server:

1. Log in as root user.
2. Navigate to *IC_INSTALL_DIR*/IC73/bin.
3. Execute the following command:

   chown root cvlansrv
4. Execute the following command to verify that the SUID bit is set on cvlansrv:

   ls -l cvlansrv
5. Execute the following command:

   crle -s *IC_INSTALL_DIR*/IC73/**lib**

Setting up Business Advocate

This section includes the following topics:

- Required administrator privileges for Business Advocate on page 51
- Prerequisites for Business Advocate on page 52
- Sharing the nethome directory on page 52
- Configuring a Business Advocate environment on page 53
- Building the database schema for the first Logical Resource Manager on page 54
- Building the database schema for an additional Logical Resource Manager on page 58
- Verifying permissions for running OA ECB with Business Advocate on page 61
- Installing Advocate Component Manager on a separate system on page 61

For information about Business Advocate components and how to configure Business Advocate, see *IC Business Advocate Configuration and Administration*.

Important:
The Resource Manager server and Resource Manager components are supported only on Windows platform that are supported by IC server. For more information, see *Avaya IC Installation Planning and Prerequisites*.

Required administrator privileges for Business Advocate

The following table describes the administrator privileges required to install, configure, and run Business Advocate components on server systems:

Implementation mode	Required administrator privileges
Workgroup mode	Administrative user with "Logon as Service" privileges
Active Directory mode	Active Directory user with local server administrator rights and "Logon as Service" privileges

Note:
To install the Business Advocate components on Windows 7, Windows 8.1 Professional, Windows 2008 R2, or Windows Server 2012 R2 operating system, you must be logged in as a Local Administrator or Domain Administrator.

Prerequisites for Business Advocate

You can set up Business Advocate only if you complete all the prerequisites including the installation of Avaya IC.

Before you install Business Advocate components, do the following:

1. Complete all prerequisites for Business Advocate, as described in *Avaya IC Installation Planning and Prerequisites*.
2. Install the IC server and administration components on a target system. For more information, see Installing IC server components on page 35.

Tip:
For Business Advocate systems that include Standby Resource Manager servers or Administration Tools on a remote server from the Resource Manager server, see *Avaya IC Installation Planning and Prerequisites* for additional configuration details.

Sharing the nethome directory

The IC Windows installer creates the `nethome` directory for Business Advocate in the *`IC_INSTALL_DIR`*`\IC73\` directory. On a system, which is hosting the first Logical Resource Manager, you must share the `nethome` directory with the required privileges for Business Advocate to function correctly.

To share the `nethome` directory:

1. In Windows Explorer, share the nethome directory as **Nethome**.
2. Change the permissions on the share to provide Read and Write permissions for the Business Advocate administrative users.

Configuring a Business Advocate environment

You must configure a Business Advocate environment on all systems that host:

- First Logical Resource Manager
- Standby Resource Manager
- Additional Logical Resource Manager
- Business Advocate administration tools

To create the Business Advocate environment:

1. Log in to the system with an account that has the required administrator privileges. For more information, see Required administrator privileges for Business Advocate on page 51.
2. Select **Start** > **Programs** > **Avaya Interaction Center 7.3** > **Advocate Configure**.

   If the Configuration Tool displays a message box that alerts you to a missing license, click **OK**. Verify that your IC license includes Business Advocate.
3. In the **Configuration** dialog box, select one of the following options from the **Configuration Type** group:
   - First Logical Resource Manager
   - Stand-By Resource Manager
   - Additional Logical Resource Manager
   - Administrative Client
4. In the **Nethome Share** field, type the path for the shared nethome directory in UNC format.

   UNC format is `\\<system_name>\nethome`

   Note:

   For Stand-By Resource Manager, specify the nethome location of the First Logical Resource Manager in the **Nethome Share** field.

   UNC format is `\\<system_name>\nethome`

   If you do not know the path, click **Browse** and navigate to the directory through Network Neighborhood. If the shared nethome directory is on the same system, do not select the local system directly. You must navigate through Network Neighborhood to ensure that the Browse function uses UNC format.

5. In the **Windows User** group, complete the following fields:
   a. In the **Domain\Username** field, type the domain and username of the user account that you created to run Business Advocate services in the following format:

Implementation mode	Domain\Username format
Workgroup mode	<*local_system_name*>\<*advocate_administrative_account*>
Active Directory mode	<*Active_Directory_domain*>\<*advocate_administrative_account*>

   b. In the **Password** field, type the password for the Active Directory user account.
   c. In the **Confirm password** field, re-type the password.
6. Click **Start**.
7. The next step depends upon the Business Advocate components you want to host on the target system. Perform one of the following steps:

Business Advocate component	Location of steps
First Logical Resource Manager	Building the database schema for the first Logical Resource Manager on page 54
Additional Logical Resource Manager	Building the database schema for an additional Logical Resource Manager on page 58

Building the database schema for the first Logical Resource Manager

To build the Business Advocate database schema for the first Logical Resource Manager, follow the steps in one of the following topics:

- Building the Business Advocate database schema for SQL Server on page 55
- Building the Business Advocate database schema for Oracle on page 56

Note:
Business Advocate databases do not support DB2.

Building the Business Advocate database schema for SQL Server

To build the Business Advocate database schema for SQL Server:

1. In the **Build Database Schema** window, enter the information for the fields mentioned in the following table.

Field	Recommended entry	Notes
Select a DBMS	Select SQL Server.	
Username	Type a DBA user name for the Business Advocate databases.	For example, a DBA user name for SQL Server is **sa**.
Password	Type the password for the DBA user name.	Do not leave your DBA password blank.

2. Check the **Build** box next to the **Local System Store** field and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Schema file	Accept the default.	Business Advocate automatically completes this field with the network home directory that you specified during installation.
Database Server	Type the name of the system that hosts the database.	The database server is the system that hosts the Business Advocate database you created when you completed prerequisites.
Database Name	Type advocate.	The database name is the Business Advocate database you created when you completed prerequisites.

3. Check the **Build** box next to the **Shared Resource Store** field and enter the information for the fields mentioned in the following table.

Field	Recommended entry	Notes
Schema file	Accept the default.	Business Advocate automatically completes this field with the network home directory that you specified during installation.
Database Server	Type the name of the system that hosts the database.	The database server is the system that hosts the Business Advocate database you created when you completed prerequisites.
Database Name	Type advocate.	The database name is the Business Advocate database you created when you completed prerequisites.

4. Click **Create Schema**.

   This process can take a few minutes to complete the installation and configuration of the database schema. Monitor the messages on the status line at the bottom left of the **Build Database Schema** window. If required, select **View Log File** to view the log file.

Building the Business Advocate database schema for Oracle

To build the Business Advocate database schema for Oracle:

1. In the **Build Database Schema** window, enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Select a DBMS	Select Oracle.	Business Advocate databases do not support DB2.
Username	Type a DBA user name for the Business Advocate databases.	For example, a DBA user name for Oracle is **system**.
Password	Type the password for the DBA user name.	Do not leave your DBA password blank.

2. Select the **Build** check box next to the **Local System Store** field and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Schema file	Accept the default.	Business Advocate automatically completes this field with the network home directory that you specified during installation.
Database Server	Type the name of the system that hosts the database.	The database server is the system that hosts the Business Advocate database you created when you completed prerequisites.
Service	Type the Oracle Local Net Service for the system.	For information on how to identify the Oracle Local Net Service, see the documentation provided by Oracle.

3. Select the **Build** check box next to the **Shared Resource Store** field and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Schema file	Accept the default.	Business Advocate automatically completes this field with the network home directory that you specified during installation.
Database Server	Type the name of the system that hosts the database.	The database server is the system that hosts the Business Advocate database you created when you completed prerequisites.
Service	Type the Oracle Local Net Service for the system.	For information on how to identify the Oracle Local Net Service, see the documentation provided by Oracle.

4. Select **Create Schema**.

   This process can take a few minutes to complete the installation and configuration of the database schema. Monitor the messages on the status line at the bottom left of the **Build Database Schema** window. If required, click **View Log File** to view the log file.

Building the database schema for an additional Logical Resource Manager

To build the Business Advocate database schema, follow the steps in one of the following topics:

- Building the Business Advocate database schema for SQL Server on page 58
- Building the Business Advocate database schema for Oracle on page 59

Building the Business Advocate database schema for SQL Server

To create the Business Advocate database schema:

1. In the **Build Database Schema** window, enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Select a DBMS	Select SQL Server.	
Username	Type a DBA user name for the Business Advocate databases.	For example, a DBA user name for SQL Server is **sa**.
Password	Type the password for the DBA user name.	Do not leave your DBA password blank.

2. Type the location of the shared network home directory that you created for the first Logical Resource Manager.

   Use UNC format, for example, `\\<system_name>\nethome`

   If you do not know the path, click **Browse** and navigate to the directory through Network Neighborhood. If the shared network home directory is on the same system, do not select the local system directly. You must navigate through Network Neighborhood to ensure that the Browse function uses UNC format.

Note:

For Additional Logical Resource Manager configuration, create a new database for example, `advocate_lrm2`, by performing the same procedure used to create database for the first Logical Resource Manager.

3. Select the **Build** check box next to System Store and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Schema file	Accept the default.	Business Advocate automatically completes this field with the network home directory that you specified during installation.
Database Server	Type the name of the system that hosts the database.	The database server is the system that hosts the Business Advocate database you created when you completed prerequisites.
Database Name	Type advocate_lrm2	The database name is the Business Advocate database, you created for additional resource manager when you completed prerequisites.

4. Click **Create Schema**.

   Monitor the messages on the status line at the bottom left of the **Build Database Schema** window. If required, click **View Log File** to view the log file.

5. Click **Close**.

6. Click **OK** for each of the dialog boxes displayed by the Business Advocate installation.

   This process can take a few minutes to complete the installation and configuration of the database schema.

Building the Business Advocate database schema for Oracle

To create the Business Advocate database schema:

1. In the **Build Database Schema** window, enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Select a DBMS	Select Oracle.	
Username	Type a DBA user name for the Business Advocate databases.	For example, a DBA user name for Oracle is **system**.
Password	Type the password for the DBA user name.	Do not leave your DBA password blank.

2. Type the location of the shared network home directory that you created for the first Logical Resource Manager.

   Use UNC format, for example, `\\<system_name>\nethome`

   If you do not know the path, click **Browse** and navigate to the directory through Network Neighborhood. If the shared network home directory is on the same system, do not select the local system directly. You must navigate through Network Neighborhood to ensure that the Browse function uses UNC format.

3. Select the **Build** check box next to System Store and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Schema file	Accept the default.	Business Advocate automatically completes this field with the network home directory that you specified during installation.
Database Server	Type the name of the system that hosts the database.	The database server is the system that hosts the Business Advocate database you created when you completed prerequisites.
Service	Type the Oracle Local Net Service for the system.	For information on how to identify the Oracle Local Net Service, see the documentation provided by Oracle.

4. Click **Create Schema**.

   Monitor the messages on the status line at the bottom left of the **Build Database Schema** window. If required, click **View Log File** to view the log file.

5. Click **Close**.

6. Click **OK** for each of the dialog boxes displayed by the Business Advocate installation.

   This process can take a few minutes to complete the installation and configuration of the database schema.

Verifying permissions for running OA ECB with Business Advocate

The Event Collector Bridge (ECB) receives information from Business Advocate on a private MSMQ called **pa_admin**. OA uses this information to report on Business Advocate.

To enable the primary ECB and the standby ECB to use the pa_admin MSMQ, the user ID that runs the IC ORB Service must have the correct permissions.

To enable OA ECB on Business Advocate, verify that the permissions on the pa_admin MSMQ are set to **Allow** for **Everyone** for the following:

- Receive Message
- Peek Message
- Get Properties
- Get Permissions

Installing Advocate Component Manager on a separate system

Advocate Component Manager and Net Home are installed on the system when the first Resource Manager (RM) is configured. However, using the following steps, you can install Advocate Component Manager and Primary and Secondary Resource Manager on separate system. Installing these components on separate systems provides high availability and better failover for Resource Manager.

Scenario

Let us consider three systems:

System 1 with Advocatecm: This system hosts the Component Manager and NetHome which is required for Administrative Clients.

System 2 with Advocateprimaryrm: This system is used to deploy the First LRM (primary role).

System 3 with Advocatestandbyrm: This system is used to deploy the Standby LRM (secondary role).

To install Advocate Component Manager on a separate system:

1. Perform the following on the Advocatecm system:
   a. Run the **BAConfigtool.exe** tool.

b. In the **Configuration** window, under **Configuration Type**, select **First Logical Resource Manager**.

c. Under **Nethome Share (\\<hostname>\nethome format)**, type **\\Advocatecm\nethome**.

d. Under Windows User, provide appropriate username and password.

e. Click **Start**.

2. Perform the following on the Advocateprimaryrm system:

a. Run the **BAConfigtool.exe** tool.

b. In the **Configuration** window, under **Configuration Type**, select **Stand-By Resource Manager**.

c. Under **Nethome Share (\\<hostname>\nethome format)**, type **\\Advocatecm\nethome**.

d. Under Windows User, provide appropriate username and password.

e. Click **Start**.

Note:

If the configtool gives an error, then run the following command from the *IC_INSTALL_DIR*\IC73*bin* path: *Mxcomponentmgr.exe /regserver*

3. Perform the following on Advocatecm system:

a. Open the Advocate Supervisor application.

b. Expand Component Manager.

c. In the left hand side pane, under **Advocate Component Manager**, select **Advocatecm**.

d. In the right hand side pane, right-click **Avaya Business Advocate Resource Manager** and click **All Tasks** > **Disable**.

e. In the left hand side pane, under **Advocate Component Manager**, select **Advocateprimaryrm**.

f. In the right hand side pane, right-click **Avaya Business Advocate Resource Manager** and click **Availability Config**.

g. In the Availability Config window, change the Availability Config from **Secondary** to **Primary**.

4. Perform the following on the Advocatestandbyrm system:

a. Run the **BAConfigtool.exe** tool.

b. In the **Configuration** window, under **Configuration Type**, select **Stand-By Resource Manager**.

c. Under **Nethome Share (\\<hostname>\nethome format)**, type **\\Advocatecm\nethome**.

d. Under Windows User, provide appropriate username and password.

e. Click **Start**.

Note:
If the configtool gives an error, then run the following command from the *IC_INSTALL_DIR*\IC73*bin* path: *Mxcomponentmgr.exe /regserver*

5. Configure two Resource Managers in the ICManager, one pointing to Advocateprimaryrm (select the Host IP of the Advocateprimaryrm) and the other pointing to Advocatestandbyrm.
6. Start both the Resource Managers.

For more details regarding BAConfigtool.exe, refer to Configuring a Business Advocate environment on page 53.

Installing the IC server SDK

IC provides a Software Development Kit (SDK) for the IC servers. The SDK includes all of the files that you require to build your own Avaya IC servers, including:

- Header files
- Libraries
- Sample server project files

Tip:
For information about how to install the Client SDK, see Installing IC server components on page 35.

To install the server SDK:

1. Navigate to the following directory in the Avaya Interaction Center CD/DVD-ROM:

Operating system	Directory path
Windows	<*CD/DVD-ROM*_drive>\Utils\TSSdk\sdkwin32.zip
Solaris	<*CD/DVD-ROM*_drive>/Utils/TSSdk/sparc_tr.Z
AIX	<*CD/DVD-ROM*_drive>/Utils/TSSdk/rs6k_tr.Z

2. Copy the compressed SDK file to your IC directory.
3. Uncompress the file and extract the contents.
4. Verify that the files have been extracted into the folder that you selected. This folder should include IC files and a makefile.

For more information, see *Avaya IC Client and Server Programmer Design Guide*.

Upgrading IC

For information on how to upgrade your IC system from an earlier release of IC, including an IC 7.x release, see *IC/OA Software Upgrade and Data Migration*.

Reinstalling IC components

You can reinstall IC Release 7.3.x over an existing IC Release 7.3.x installation. To uninstall IC files before you reinstall, see Uninstalling IC on page 496.

To reinstall IC over an existing IC installation:

1. Stop all IC servers and IC services on the target system.
2. Follow the instructions in the appropriate section below to reinstall the required IC files:
   - Installing IC server components on page 35
   - Deploying Avaya Agent on page 398
   - Installing Avaya Agent Web Client on page 444

Upgrading Daylight Saving Time (DST) patches

Avaya IC is compliant with Daylight Saving Time (DST).

The major operating system (OS) vendors have already released patches to support DST. Avaya IC customers must upgrade their operating system versions with the required DST patches from the respective operating system vendor's Web sites.

You can update the JRE on all the platforms using third-party tools.

For example:

- **TZUpdater**
- **TZUpdater**
- **JTZU**

To update JRE using the Java Time Zone Updater tool:

1. Stop all Avaya IC servers, services and log out Avaya Agent.
2. Update JRE that comes with Avaya IC.
   - You can download the Java Time Zone Updater (**TZUpdater**) tool from the Oracle website. For instructions on installing **TZUpdater**, refer to the Oracle website.
   - You can download and install the **TZUpdater** (Java Time Zone Updater) tool from Oracle website. For instructions on installing TZUpdater, refer to the Oracle website.
   - You can download the **JTZU** (Java Time Zone Updater) tool from the IBM website. For instructions on installing JTZU, refer to IBM website.

Note:

- JRE is located in the *IC_INSTALL_DIR*\IC73\Java directory.
- If you are changing the time zone after installing and configuring IC, update the adl files, such as `repository.adl`, `ccq.adl` and regenerate the database.

Comments on this document? infodev@avaya.com

Chapter 4: Silent Install Interaction Center 7.3

Avaya IC uses Install Anywhere platform for RTM installers. You can install Avaya IC 7.3 in silent mode in the following two ways:

- Option 1: Run the installer with default values (no response file)
- Option 2: Using a response file to supply values for installer variables

Option 1: Run the installer with default values (no response file)

To run the installer with the default values:

1. Open command prompt on Windows system.
2. Open shell prompt on Unix system.
3. Go to the installer directory where the installer is copied.
4. At the shell command prompt, run the commands given in the following table:

Operating System	Command
Windows	To install the application with the required Visual C++ Runtime: **`install.exe –i silent -D$CHOSEN_DIALOG_BUTTON_FORVCREDIST$=0`** OR To install the application without the required Visual C++ Runtime: **`install.exe –i silent -D$CHOSEN_DIALOG_BUTTON_FORVCREDIST$=1`**
Oracle Solaris	**`./install.bin -i silent`**
IBM AIX	**`./install.bin -i silent`**

Note:

There are multiple install sets within some installers, for example, icwinserversuite contains Server, Design/Admin, and AAWC. Only the 'default' install set will be installed when the installer is run without using a response file. Table 2 lists the default Install set for multi-set installer in Avaya IC. Use this option only if the default install set needs to be installed.

Avaya IC Installer	Install Set	Default Install set
icwinserversuite	Server, Design and Admin, and Web Connector	Server
icclientsuite	Avaya Agent Rich Client and Avaya Agent Web Client	Avaya Agent Rich Client
SiebelNT	ASServer and ASDesign	ASServer
icsolserversuite	Server, Web Connector	Server
icaixserversuite	Server, Web Connector	Server

Option 2: Using a response file to supply values for installer variables

To use a response file to supply values for installer variables:

1. Create a response file.
   a. Open the shell command prompt on the system.
   b. Go to the installer directory where you copied the installer.
   c. At the command prompt:
      - Execute the commands in the following table to create the default `installer.properties` response file in installer directory:

Operating System	Command
Windows	**`install.exe -r`**
Oracle Solaris	**`./install.bin -r`**
IBM AIX	**`./install.bin -r`**

Comments on this document? infodev@avaya.com

- Execute the commands in the following table to create the default `installer.properties` response file at the specified file location.

Operating System	Command
Windows	To install the application with the required Visual C++ Runtime: **install.exe -i silent -f** <absolutepathoffile.txt> **-D$CHOSEN_DIALOG_BUTTON_FORVCREDIST$=0** OR To install the application without the required Visual C++ Runtime: **install.exe -i silent -f** <absolutepathoffile.txt> **-D$CHOSEN_DIALOG_BUTTON_FORVCREDIST$=1**
Oracle Solaris	**./install.bin -i silent -f**<abosolute_path_of_file.txt>
IBM AIX	**./install.bin -i silent -f**<abosolute_path_of_file.txt>

d. Installer launches after executing the above command. Change the default values in the response file as per your requirement.

e. Save the file.

2. Modify the response file.

Note:

This step is required for the installers mentioned in the Option 1: Run the installer with default values (no response file) section.

a. After the installation is complete, a response file is created in the same directory where the installer is located or at the absolute path location if specified.

b. Open the response file in a text editor.

c. Add the lines provided in the Data column from the following table in the response file for the respective installation. This step is required for all Avaya IC installers that have multiple install sets. Refer to Table 2. The values related to install set are not written to the response file. This is a known issue of IA 2009.

d. Save and close the file.

Installer	Data
Windows Server	#Choose Install Set #---------- CHOSEN_FEATURE_LIST=Servers CHOSEN_INSTALL_FEATURE_LIST=Servers CHOSEN_INSTALL_SET=Custom
Windows design and Admin	#Choose Install Set #---------- CHOSEN_FEATURE_LIST=DesignA CHOSEN_INSTALL_FEATURE_LIST=DesignA CHOSEN_INSTALL_SET=Custom
Windows WebConnector	#Choose Install Set #---------- CHOSEN_FEATURE_LIST=WebConn CHOSEN_INSTALL_FEATURE_LIST=WebConn CHOSEN_INSTALL_SET=Custom
Solaris Server1	#Choose Install Set #---------- CHOSEN_FEATURE_LIST=servers CHOSEN_INSTALL_FEATURE_LIST=servers CHOSEN_INSTALL_SET=Custom
Solaris WebConnector1	#Choose Install Set #---------- CHOSEN_FEATURE_LIST=WebConn CHOSEN_INSTALL_FEATURE_LIST=WebConn CHOSEN_INSTALL_SET=Custom
AIX Server1	#Choose Install Set #---------- CHOSEN_FEATURE_LIST=servers CHOSEN_INSTALL_FEATURE_LIST=servers CHOSEN_INSTALL_SET=Custom

Installer	Data
AIX WebConnector1	#Choose Install Set #---------- CHOSEN_FEATURE_LIST=WebConn CHOSEN_INSTALL_FEATURE_LIST=WebConn CHOSEN_INSTALL_SET=Custom
AIC Siebel Windows (AICSiebelNT)	Server: #Select Installer options #---------- CHOSEN_FEATURE_LIST=ASServer CHOSEN_INSTALL_FEATURE_LIST=ASServer CHOSEN_INSTALL_SET=Custom Design: #Select Installer options #---------- CHOSEN_FEATURE_LIST=ASDesign CHOSEN_INSTALL_FEATURE_LIST=ASDesign CHOSEN_INSTALL_SET=Custom
Windows WebClient	#Select Installer options #---------- CHOSEN_FEATURE_LIST=AAWC CHOSEN_INSTALL_FEATURE_LIST=AAWC CHOSEN_INSTALL_SET=Custom
AICSiebel Solaris	N/A
AICSiebel AIX	N/A
Windows AgentClient	N/A
Siebel Windows	N/A
Siebel Solaris	N/A
Siebel AIX	N/A

Note:

[1] This is specific to Solaris/AIX platform. Open the response file to edit and remove the trailing `Avaya/IC73` path from the `USER_INSTALL_DIR` path variable value, because during installation, the `Avaya/IC73` directory structure is appended to the path.

N/A – Not Applicable. No install sets.

Rows starting with '#' are treated as comments.

3. You can now run the installer on a different system (where installation is required).
   a. Go to the installer directory.
   b. Open the command/shell prompt and run the following command:

Operating System	Command
Windows	**install.exe -i silent -f**<abosolute_path_of_file.txt>
Oracle Solaris	**./install.bin -i silent -f**<abosolute_path_of_file.txt>
IBM AIX	**./install.bin -i silent -f**<abosolute_path_of_file.txt>

Comments on this document? infodev@avaya.com

Chapter 5: Configuring core servers

Avaya IC installation copies all IC server files to the target system. You cannot copy the files for selected servers on a system. If your IC configuration requires only certain servers on a system, run the IC installation on that system to copy the server files. You must then configure only those servers that you want to host on the system.

This section describes how to configure the core servers, including the IC domains and accounts required for these servers. This section includes the following topics that provide the steps that you need to follow to configure the core servers:

1. Before you configure IC core servers on page 72
2. Using IC domains on page 73
3. Setting up administrative accounts on page 77
4. Using system and sample workflows on page 82
5. Configuring core servers on page 83
6. Starting and stopping IC servers on page 107
7. Starting and stopping IC services on page 114

Before you configure IC core servers

Before you configure the IC core servers, ensure that you:

1. Install and configure all the prerequisite software and hardware. For more information, see *Avaya IC Installation Planning and Prerequisites*.
2. Copy the IC server files to the target systems. For more information, see Installing IC server components on page 35.
3. Configure the server environment. For more information, see Configuring the ORB server environment on page 44.
4. Configure the IC databases. For more information, see Configuring databases on page 122.

Creating sites

A site is a physical location that agents or servers can occupy in an IC system. For a single site system, you can use the Default site that is pre-configured.

For an IC system that includes multiple physical locations, create a site for each physical location. The site name must identify the physical location. IC uses the site information for routing decisions. For more information, see *Interaction Center Administration Guide*.

To create a site:

1. In IC Manager, select **Tools** > **Site**.
2. In the **Site Editor** dialog box, click **New**.
3. In the **Create Site** dialog box, enter the information for the following fields:
   a. **Name:** Enter the name for the site that identifies the physical location.
   b. **Description:** Enter the description of the site.
4. Click **OK**.
5. In the **Site Editor** dialog box, Click **OK**.

Using IC domains

At a minimum, an IC system should include the pre-configured domains installed with IC. Create multiple IC domains for your servers and agents to increase performance and allow IC to handle higher contact rates. For example, use a Voice domain for the servers used for Telephony.

To use domains, review and perform the steps in the following topics:

1. Preconfigured domains on page 74.
2. Guidelines for IC domains on page 75.
3. Creating domains on page 76.
4. Establishing the failover order for domains on page 76.

Preconfigured domains

IC includes several domains that are pre-configured with failover paths. The following table describes the pre-configured domains.

Preconfigured domain	Members	Failover path
Default	• Alarm server • Directory server • License server • ORB server	• Default
Email	None	• Email • Email_Helper • Web • Default
Email_Helper	None	• Email_Helper • Email • Default
Prompter1	None	• Prompter1 • Default • Voice1
User1	None	• User1 • Prompter1 • Voice1 • Default • Email • Email_Helper • Web • Web_Helper
Voice1	None	• Voice1 • Default
Web	None	• Web • Web_Helper • Email • Default

Preconfigured domain	Members	Failover path
Web_Helper	None	• Web_Helper • Web • Default
Website	None	• Website • Web • Voice1 • Default

Guidelines for IC domains

The IC domains can span servers at different locations and multiple domains can share the same server. A failover order is associated with each domain. The failover order defines how the members of a domain fails over to the servers in other domains. If a server in one domain becomes unavailable, the requests to that server are routed to a server in the failover domain.

Tip:
Plan your failover policy carefully. If you specify a failover domain at a remote site, you must ensure that you have a high-bandwidth connection between the two sites. Otherwise, system performance might be adversely affected.

Consider the following guidelines while selecting the domains you need in your Avaya IC environment:

- Use logical names that include identifying information, such as the site, the media channel, or the agent workgroup.
- Set up the failover paths for domain, that include agents, to ensure that the domains failover to one or more domains with an ORB server, Alarm server, and Directory server. If the domains that contain agents do not failover to domains with these servers, then Avaya Agent cannot function correctly.
- Do not assign an agent or a server to more than one domain. If you assign an agent or server to a second domain, IC Manager automatically deletes that agent or server from the first domain.
- Do not associate multiple servers of the same type with the same domain, with the possible exception of the ORB server. You can have multiple ORB servers in the same domain if those servers reside on different hosts.
- Assign agents to User domains.
- Divide your agents between two User domains.

If you configure the failover of each User domain to the other domain, then you have a minimum amount of interruption if a Blender server or agent Workflow server fails.

For examples of how to divide IC servers between domains, see *Avaya IC Installation Planning and Prerequisites*. For more information about domains and failover, see *Interaction Center Administration Guide*.

Creating domains

You can add as many domains as you need to handle the agents and servers in your IC system. For suggested deployments, see *Avaya IC Installation Planning and Prerequisites*.

CAUTION:
Do not delete the Default domain. Avaya IC requires the Default domain to function.

To create a domain:

1. On the IC Manager toolbar, click **Domains**.
2. In the **Domain Manager**, Select **Servers** under the **Items** section.
3. In the left pane, select and right-click **All Domains** and select **New**.
4. Enter the new domain name.

   The domain name can have a maximum of 32 characters, and must start with alphabetic characters. You can use underscores in the domain name but you cannot use spaces.
5. Click **OK**.

   The system adds the new domain name under the **All Domains** list in the left pane.

Establishing the failover order for domains

If a server becomes unavailable, failover redirects all requests from the clients of the unavailable server to an alternative server in a failover domain. A server's client can be an agent desktop application or another server.

A client or a server logs in to the IC system by invoking a `DS.Login` request. When the `DS.Login` request is invoked, there is no information available to identify the group of the client or domain of the server that is making the request. The IC components assume that the request has come from the Default domain.

While membership in a domain determines how the domain members communicate to servers, membership also defines how failover is performed. You must pre-plan your server failover strategy before proceeding.

You must ensure that your failover plan follows the deployment guidelines, including:

User domain failover: If your User domain does not include a secondary ORB server, the User domain must failover to a domain that includes an ORB server, such as the Default domain.

Data server failover: When an agent logs in to the Avaya IC system, Avaya IC cannot determine the agent's assigned domain until the login request succeeds. Therefore, during the login process, IC components assume that all agents belong to the Default domain. To ensure that the Data servers handling login requests failover correctly, these servers must include the Default domain in their server group.

IC Email server failover: The domain that includes your IC Email server must failover to the domain that includes your WebACD server.

WebACD server failover: The domain that includes your WebACD server must failover to the domain that includes your IC Email server.

For more suggestions on how to plan your failover strategy, see the deployment scenarios in *Avaya IC Installation Planning and Prerequisites*. You can also establish failover order on a server-by-server basis. For more information, see *Interaction Center Administration Guide*.

To establish the failover order for a domain:

1. In the Domain Manager, select **Servers** in the **Items** section.
2. In the left pane, select a domain for which you want to establish failover.
3. In the right pane, click the **Fail Over** tab.
4. Select the failover domain from the **Available** list.
5. Click **Add** to move the selected domain to the **Members** list.

   You can select multiple domains to add them to failover members. IC uses these failover domains in the specified order. Use Up and Down arrows located above the **Members** list to rearrange failover order. Do not move a failover domain above the primary domain.
6. Click **Ok**.

Setting up administrative accounts

IC requires two types of administrative accounts:

Human users: These administrative accounts are reserved for human IC users, such as supervisors and managers. For more information, see Using administrative accounts for human users on page 80.

Non-human users: These administrative accounts are reserved for non-human IC users, such as servers and IVRs. For more information, see Using administrative accounts for non-human users on page 78.

This section describes the minimum number of administrative accounts that are required to install and configure IC, and how to create those accounts. Topics include:

- About IC passwords on page 78.

- Using administrative accounts for non-human users on page 78.
- Using administrative accounts for human users on page 80.
- Creating administrative accounts on page 80.

For more information about administrative and agent accounts, see *Interaction Center Administration Guide*.

About IC passwords

All IC accounts, including administrative accounts and accounts for non-human users, must have passwords. The password must meet the requirements specified in the Agent/Security properties for the workgroup or for individual agents.

These requirements include:

- Maximum length
- Minimum length
- Minimum number of alphabetic characters
- Minimum number of numeric characters

For more information, see *Interaction Center Administration Guide*.

Using administrative accounts for non-human users

The IC components, such as the Configuration Tool and some servers, require administrative accounts. These accounts should not be used by a human IC user.

Important:
Configure all IC accounts for non-human users such that the password for these accounts never expire or change.

These administrative accounts are non-human accounts for IC components only. You do not need to create these accounts in the User domain. When you create an administrative account for an IC server or component, such as the ICM server, the account must be in either of the following domains:

- The same domain as the component that uses the account.
- A domain in a failover path from the domain of the component.

The following table describes the minimum number of administrative accounts your IC system requires for non-human IC users.

Important:
If you plan to use an account created by the seed data, you must change the password for that account.

Account	Component	Description	Login
New account	Avaya IC servers	Create an administrative account in: • The same domain as the component that uses the account. OR • A domain in a failover path from the domain of the component. **Note:** Do not use the Admin account created by the seed data, or an account that you use to log in to IC Manager.	As defined by user. Not available in seed data.
Admin	IC Manager login	Administration account that you use to log in to the Configuration Tool and IC Manager when you configure IC. Domain: User1 Role: Administrator **Note:** IC Manager forces you to change the password for this account.	Login: Admin Password: admin
website	Configuration Tool and IC servers	You use this account to configure the Website Web application and Web Management services. The IC components in the DMZ use this account to access other IC servers and components. Domain: Website Role: Operator	Login: website Password: website

Account	Component	Description	Login
icmbridge	ICM Bridge	You use this account to configure the Attribute server. For more information, see Creating the Attribute server on page 200. Include a Workflow server in the same domain as the ICM account. Domain: Web Role: Operator	Login: icmbridge Password: icmbridge
dcobridge1	DCO Bridge	The Java Application Bridge uses this account to access IC servers, such as the Data server. Each Java Application Bridge in an IC system requires a unique DCO Bridge account. Domain: User1 Role: Agent	Login: dcobridge1 Password: dcobridge1

Using administrative accounts for human users

All human IC users who require administrative privileges, such as access to IC Manager and other Design and Administration Tools, require administrative accounts. These accounts should not be used by a non-human IC user. IC user must regularly change the password for these accounts.

Important:
When you create an administrative account for a human IC user, the account must be in the User domain.

You can create an Administration domain that is restricted to administrative accounts for human users.

Creating administrative accounts

You must create a domain for the administrative accounts before you perform these steps.

You may want to create an additional administrative account in the User domain that can communicate with the parent directory server. This additional account is useful if you have a problem with the configuration of one or more domain. After you configure the additional account, log in to IC Manager using that account and confirm that you can use the account for administrative access.

To create administrative accounts:

1. In IC Manager, click the **Agent** tab.
2. In the left pane, select **Administrator**.

   If **Administrator** is not visible, select **Manager** > **Refresh** to update the information.
3. Select **Agent** > **New**.
4. Click the **General** tab and enter the information for the fields mentioned in the following table:

Field	Description
First Name	Required field Type agent's first name.
Last Name	Required field Type agent's last name.
Preferred Name	Required field Type agent's preferred name.
Employee ID	Type the agent's company employee ID. This step is optional.
Login ID	Required field Type a login ID that the agent uses for all IC applications.
Domain	Required field Select the appropriate domain from the list.
Task Load	Required field Set to 0.
Task Ceiling	Required field. Set to 0.
Site	Select a site from the drop-down list. **Note:** IC uses the Site to compile statistics for groups or agents or queues.

5. Click the **Security** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry
Password	Type the password for this account.
Confirm	Re-type the password for this account.

Field	Recommended entry
Force password change on login	Perform one of the following: • Select this field for human IC users. • Do not select this field for non-human IC users.
Disable login	Do not select this field.
Administrator	Select this field. **Note:** Do not select any of the other roles.

6. Click **Ok**.

Using system and sample workflows

When you install Workflow Designer, you also install system and sample workflows. IC installs the project folders for system and sample workflows in subfolders of the following directory:

IC_INSTALL_DIR\IC73\design\IC\Flows\Avaya

CAUTION:
Do not change a system workflow. If you change a system workflow, one or more components of your IC system may not function correctly.

Sample workflows

The following table describes the sample workflows for IC:

Workflow project	Description
Blender	Required for all installations.
ICEmail	Required for installations that include Email Management.
Prompter	Required for installations that include Prompter.
TS	Required for all installations that include Telephony.
WACD	Required for all installations that include Web Management or Email Management.

For a complete list of the workflows in these projects, including the directories where IC installs the workflows, see *Avaya IC Workflow Designer User Guide*.

Using sample workflows

You can use sample workflows to set up and test your IC system. When you test your system, review the settings of the sample workflows for the media channels and components in your IC system.

You can customize sample workflows to meet the business requirements of your contact center. For example, the Email Analysis flow in the ICEmail project contains sample routing hints for testing purposes. You must review and change these properties to the routing hints that meet the needs of the contact center.

After you customize the sample workflows, recompile the workflows and load them in a database. For more information, see *Avaya IC Workflow Designer User Guide*.

Workflows in IC seed data

The IC seed data includes compiled system and sample workflows for all projects. When you create the CCQ database, you import the compiled workflows with the seed data and store them in that database.

You must update some of these workflows, such as the workflows in the TS project before you can use them in your IC. For more information, see *Avaya IC Workflow Designer User Guide*.

Configuring core servers

The IC installation program automatically creates some of the core servers when you install the IC servers and administration components. For more information, see Installing IC server components on page 35.

Important:
You have to be careful when you modify the server configuration parameters. Errors can seriously impact the performance of your IC system.

This section describes the procedures to configure the remaining core servers. You have already created and configured some core servers. Before you configure media channels and media-specific servers, perform the steps in the following topics to configure the remaining core servers:

- Server naming guidelines on page 84.

- Recommended tuning parameters for IC servers on page 85.
- Creating an ADU server on page 85.
- Creating a DUStore server on page 86.
- Creating an EDU server on page 91.
- Creating a Report server on page 93.
- Creating a Workflow server on page 94.
- Creating a Blender server on page 98.
- Creating an HTTP Connector server on page 100.
- Creating a Notification server on page 103.

Note:

If you reconfigure a running server in IC Manager, stop and restart the server for the settings to take effect. Do not select the **Auto start** option until you successfully add and configure the servers and start them manually.

These topics contain information about required server parameters. For more information, see *Interaction Center Administration Guide*.

Server naming guidelines

Under certain circumstances, the Workflow server fails to connect with a server that uses the server type as the name of the server. For example, when an ADU server with the server type ADU is named as "ADU". Similarly, the Web Advocate Adaptor server with the server type as WAA is named as "WAA".

To ensure optimal functioning of your IC system, you must use the following naming conventions for your IC servers:

- Always use a unique server name, which can be up to 32 characters long without spaces.
- Name your Data servers Data_<*databasetype*>_<*domain*>. For example, **Data_Oracle_Default**.
- In a single site environment, name all other servers <*servername*>_<*domainname*>. For example: **ADU_User1**.
- In a multi-site environment, name all other servers <*servername*>_<*sitename*>_<*domainname*>. For example: **ADU_London_User1**.
- Do *not* set the server name same as the server type, or IC may encounter errors during operation. For example, use **TS_Voice1** as the name of your Telephony server, not just **TS**.

Important:
Do not use the name **localVDU** or **localADU** for EDU or ADU servers. These are used when the servers are taken off-line to prevent communication with other EDU and ADU servers.

Recommended tuning parameters for IC servers

A set of recommended tuning parameters to enhance the performance of an IC system is available in *Interaction Center Administration Guide*.

Creating an ADU server

An IC deployment includes more than one ADU server.

If the IC system includes an ADU server that handles queued ADU entries for a WebACD server, that ADU server should not accept failover requests from an ADU server that handles agent accounts. For more information, see *Interaction Center Administration Guide*.

For Business Advocate, the ADU server contains statistics for service classes.

An ADU server must be able to communicate directly with the parent Directory server. For more information about the parent Directory server, see Creating a Directory server on page 88.

To create an ADU server:

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **ADU** and Click **OK**.
3. Click the **General** tab, and enter the information for the fields mentioned in the following table.

Field	Recommended entry	Notes
Name	ADU_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Voice` from the drop-down list if the server is in the Voice domain.
Host	Select the IP address of the system from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Click the **ADU** tab.

5. In the **Idle Time (min)** field, ensure that the minutes entered are greater than the length of a shift for an agent.

   Important:
   If an agent is logged into an IC agent desktop application for longer than the idle time set in the ADU server, the ADU for the agent will time-out. An ADU time-out can cause problems such as inconsistent data in OA reports and the inability to defer email contacts. Therefore, the idle time should be longer than a typical agent shift and all agents should log out of IC at the end of a shift.

   You can use the default settings for the ADU server. For more information about the parameters, see *Interaction Center Administration Guide*.

6. Click **OK**.

Note:
Do not start the ADU server before you configure all core servers. To ensure that the servers start correctly, see Starting and stopping IC servers on page 107.

Creating a DUStore server

All IC systems that include Email Management require a DUStore server. You can also add a DUStore server for Telephony or Web Management. For more information about deployment scenarios for IC servers, see *Avaya IC Installation Planning and Prerequisites*.

The IC installation program does not automatically add this server.

To create a DUStore server

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **DUStore**, click **OK**.

3. Click the **General** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	DUStore_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the IC domain for the server from the drop-down list.	Include the DUStore server in the same domain as the EDU server for the channel. For example, select `Email_Helper` from the drop-down list if this server handles the email contacts. For more information about recommended domains, see *Avaya IC Installation Planning and Prerequisites*.
Host	Select the IP address of the system from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Click the **DUStore** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
IC Data Source	Select the Avaya IC Data Source, which is the ADL file, for the Avaya IC Repository database.	If you used the default name, select `repository`.
Default deletion age (Days)	Enter the number of days that Avaya IC holds an EDU in the absence of other information.	Default is 60 days. After this period, the DUStore deletes the EDU from the DUStore table and retires the EDU to the database.
Deleted per scan	Enter the number of EDUs the DUStore retires to the database when it scans the system for expired EDUs.	Default is 1000.

Field	Recommended entry	Notes
Scan Interval (min)	Enter the period of time, in minutes, the server scans for expired EDUs.	Default is 15. Higher values may save some CPU time; lower values make for more predictable behavior during prototyping and testing. Assume that other timers in the EDU could be off by as much as (the **Scan Interval** + 1) to start.
Purge Alarm	Select to raise an alarm if a delete scan finds any EDUs that meet the criteria for deletion and retirement to the database.	Default is selected.

5. Click **OK**.

Note:
Do not start the DUStore server before you configure all the core servers. To ensure that the servers start correctly, see Starting and stopping IC servers on page 107.

Creating a Directory server

The Directory server maintains a list of all the servers in Avaya IC. When you create multiple Directory servers, they share a common directory.

This section includes the following topics:

- Configuring the primary Directory server on page 88
- Creating a secondary Directory server on page 90

Configuring the primary Directory server

You must designate one Directory server to synchronize the directories and ensure that the changes made by one Directory server are reflected throughout the network. This designated Directory server is called the parent. If there is only one Directory server in Avaya IC, IC Manager automatically assigns parent status to the server. For more information, see the *Interaction Center Administration Guide*.

Usually, the primary Directory server is on the same system as the primary ORB server.

To configure the primary Directory server:

1. In IC Manager, click the **Server** tab.
2. Double-click the Directory server to open the Server Editor.

3. Click the **Directory** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
IC Data Source	Select the IC Repository data source from the IC Data Source drop-down list.	If you used the default name, select `repository`.
Is Parent	Select this box as this Directory server is the parent directory server.	The parent Directory server synchronizes the directories for all Directory servers.
Backup	Enter the name of a backup file to be created. This file uses a backup copy of the directory. Click Start to create the file in the home directory of the server.	Avaya IC appends an .ffd extension to the file name.
Restore	Enter the file name of the backup file used as the name of the directory you want to restore. Click Start to restore the directory.	The file name you enter must be a previously created backup directory file.
First update lag (sec)	Enter the number of seconds that the Directory server waits before sending updates to the first of its children.	During normal operation, set this value to 0. A nominal delay occurs automatically. There is no maximum value. If this value is greater than 0, the Advanced tab contains a couple with the name "PropagationDelay" and a value equal to the current buffer updates setting.
Succeeding update lag (sec)	Enter the number of seconds that the Directory server pauses before sending an update to the next child.	During normal operation, set this value to 0 or 1. There is no maximum value. If this value is greater than 0, the Advanced tab contains a couple with the name "LagBetweenChildren" and a value equal to the current childlag setting.

4. Click **OK**.
5. Stop and restart the Directory server.

Creating a secondary Directory server

To create a secondary Directory server:

1. In IC Manager, click the **Server** tab.
   a. Select **Server** > **New**.
   b. From the list of servers, select **Directory**.
   c. Click **OK**.
2. Click the **General** tab and enter the information for the fields mentioned in the following table.

Field	Recommended entry	Notes
Name	Directory_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the domain from the drop-down list.	For example, select `Default` from the drop-down list if the server is in the Default domain.
Host	Select the IP address of the system from the drop-down list, or type in a new IP address.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

3. Click the **Directory** tab and complete the fields as shown in the following table.

Field	Recommended entry	Notes
IC Data Source	Select the IC Repository data source from the IC Data Source drop-down list.	If you used the default name, select `repository`.
Is Parent	Do not select this box, as this Directory server is a secondary, or child, Directory server.	The parent Directory server synchronizes the directories for all Directory servers.
Backup	Enter the name of a backup file to be created. This file used a backup copy of the directory. Click Start to create the file in the server's home directory.	Avaya IC appends an .ffd extension to the file name.

Field	Recommended entry	Notes
Restore	Enter the file name of the backup file used as the name of the directory that you want to restore. Click Start to restore the directory.	The file name you enter must be a previously created backup directory file.
First update lag (sec)	Enter the number of seconds that the Directory server waits before sending updates to the first of its children.	During normal operation, set this value to 0. A nominal delay occurs automatically. There is no maximum value. If this value is greater than 0, the **Advanced** tab contains a couple with the name "PropagationDelay" and a value equal to the current buffer updates setting. **Note**: This is only relevant to MOMMY DS.
Succeeding update lag (sec)	Enter the number of seconds that the Directory server pauses before sending an update to the next child.	During normal operation, set this value to 0 or 1. There is no maximum value. If this value is greater than 0, the **Advanced** tab contains a couple with the name "LagBetweenChildren" and a value equal to the current childlag setting. **Note**: This is only relevant to MOMMY DS.

4. Click **OK**.
5. Copy the `ds.ffd` file from the system that hosts your primary Directory server to the system that hosts your secondary Directory server.
6. In IC Manager, start the secondary Directory server.

Creating an EDU server

Create at least one EDU server for each media type in your IC system. For example, using the pre-configured domains, if your IC system includes all three channels, create the following EDU servers:

- VoiceEDUServer in the Voice1 domain.

- WebEDUServer in the Web_Helper domain.
- EmailEDUServer in an Email_Helper domain.

The IC installation program does not automatically add these servers.

Important:
IC requires that you place each EDU server in a separate IC domain. An IC domain cannot include more than one EDU server. For more information about recommended deployment scenarios and guidelines for the EDU server, see *Avaya IC Installation Planning and Prerequisites*.

To create an EDU server:

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **EDU** and click **OK**.
3. In the **Initialize EDU** dialog box, select the media type from the drop-down list and click **OK**.
4. Click the **General** tab, and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	EDU_<*domain*>_<*media*>	Include the domain in the server name to identify the server. For example, if you must create an EDU server for voice media, type EDU_Voice1_Voice.
Domain	Select the IC domain for the server from the drop-down list.	For voice contacts, add the EDU server to the same domain as the associated Telephony server. For chat contacts and email contacts, add the EDU server to a "Helper" domain. For example, select `Email_Helper` from the drop-down list if this server handles email contacts. For more information about recommended domains, see *Avaya IC Installation Planning and Prerequisites*.
Host	Select the IP address of the system from the drop-down list, or type in the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. Click the **EDU** tab and review the default settings.

   You can use the default settings for the EDU server to get your system up and running. For more detailed information about these parameters and how to customize them for your system, see the *Interaction Center Administration Guide*.

6. Click **OK**.

Note:
Do not start this server before you configure all core servers. To ensure that the servers start correctly, see Starting and stopping IC servers on page 107.

Creating a Report server

The Report server writes values from EDUs to the IC Repository database. OA uses these values to generate historical reports.

The IC installation program does not automatically add Report server.

CAUTION:
If you set the **Server Trace Level** field to 10 on the **Debug** tab, the Report server saves text files with information about each EDU in the *IC_INSTALL_DIR*\IC73\temp directory. The Report server names these text files as <*eduid*>.txt. IC does not automatically delete these files. You must manually delete these files when they are no longer needed for debugging. If you do not reset the Server Trace Level, the files continue to accumulate in the *IC_INSTALL_DIR*\IC73\temp directory.

To create a Report server:

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **Report** and click **OK**.
3. Click the **General** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	Enter a name for the Report server. For example, Report_<*domain*>	Include the domain in the server name to identify the server.

Field	Recommended entry	Notes
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Voice1` from the drop-down list if the server is in the Voice domain.
Host	Select the IP address of the system from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Click the **Report** tab, and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
IC Data Source	Select the IC Data Source for the IC Repository database.	For example, if you used the default name to create the IC Repository application, the data source name is `repository`.

5. Click **OK**.

Note:
Do not start this server before you configure all core servers. To ensure that the servers start correctly, see Starting and stopping IC servers on page 107.

Creating a Workflow server

The IC installation program does not automatically add a Workflow server. Typically, an IC system includes more than one Workflow server.

To create the Workflow server, perform the steps in the following topics:

1. Configuring multiple Workflow servers on page 94
2. Creating a Workflow server on page 95
3. Completing the Agent Prompting Workflow server configuration on page 98

Configuring multiple Workflow servers

For a large IC system that has a high contact delivery rate and that hosts servers across multiple systems, you can distribute the workflow responsibilities across multiple Workflow servers to maximize performance and response.

For example, you can set up the following workflow servers to process contacts in the different media channels and to handle the different agent-related tasks:

Workflow server for the voice channel: Runs voice contact routing workflows to process voice contacts. These Workflow servers are in a voice domain. For more information, see Configuring a Workflow server for Telephony on page 186.

Workflow server for the chat channel: Runs web contact routing workflows to process incoming chat contacts. These Workflow servers are in a Web domain. For more information, see Configuring a Workflow server for Web Management on page 229.

Workflow server for the email channel: Runs email contact routing workflows and email analysis workflows to process incoming and outbound email contacts. These Workflow servers are in an email domain. For more information, see Configuring a Workflow server for Email Management on page 342.

Workflow server for agent prompting: Runs Prompter workflows and agent script workflows. For information on how to configure a Workflow server to run Prompter flows, see Creating a Workflow server on page 95.

Workflow server for agent searches and transfers: Runs agent search and transfer workflows for the Unified Agent Directory. These Workflow servers are in a User domain. For more information about the configuration of these servers, see Configuring a Workflow server for transfers and conferences on page 395.

Creating a Workflow server

The instructions given in this section create a basic Workflow server. You must configure this Workflow server to handle the appropriate tasks. For more information, see Configuring multiple Workflow servers on page 94. For more detailed information about parameters in the Workflow server, see *Interaction Center Administration Guide*.

To create a Workflow server:

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **Workflow**.
3. Click **OK**.
4. Click the **General** tab, and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	Workflow_<*domain*>	Include the domain in the server name to identify the server.

Field	Recommended entry	Notes
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Users1` from the drop-down list if the server is in the Users1 domain.
Host	Select the IP address of the system from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. Click the **Workflow** tab and perform the following steps:

   a. From the **IC Data Source** drop-down list, select the data source that this Workflow server uses.

      Most Workflow servers use the Interaction Center data source. The default name for this data source is interaction_center.

Note:
For a Workflow server that runs Prompter flows and agent script workflows, the IC Data Source must match the database that was used to build and store the workflows.

   b. Review the remaining fields on the tab, as shown in the following table. You must complete some of these fields, such as the **Synchronous Startup Flows**, when you create Workflow servers for specific tasks.

Field	Recommended entry	Notes
Reload Flows	Select this button to reload workflows in the Workflow server.	You can choose to update file-based workflows and workflows stored in the database, and whether to force an immediate reload rather than wait for running workflows to complete execution. Select **Force immediate reload** to reload all the currently loaded flows even if the version numbers are the same.
Unload Flow	Select this button to unload a workflow from the server. You will be prompted to enter the workflow name.	When the workflow is next requested, the latest version of the workflow will be loaded from the Database or File System. If the workflow is currently running, it will complete before being unloaded. You must manually increase the workflow version number. If the version has not been increased, the workflow is not reloaded.

Field	Recommended entry	Notes
Run Flow	Select this button to run a workflow that updates the variable that contains queue-workflow information.	Enter the workflow name. The queue-workflow information is required by contact routing flows in a Blender environment. Update the variable whenever any change is made to the queue.
IC Data Source	Select a data source from the drop-down list.	For most Workflow servers, select the Interaction Center data source. If you used the default name, select `interaction_center`.
Preload Flows	Select the Ellipsis (…) and specify the workflow to be loaded when the server is first started.	If you have a workflow that must react very quickly when the event triggering it is received by Avaya IC, use the Preload Flows option to have that flow ready and waiting in memory. When the event actually occurs, Avaya IC can run the flow without having to load it first. Syntax: *`projectname.flowname`* **Note:** Preloading a large flow can slow down server startup.
Synchronous Startup Flows	Select the Ellipsis (…) and specify the workflow to be loaded before the startup workflows and before the server accepts requests.	For example, Workflow servers that run contact routing workflows need to run web_routing.update_qw_cache as a synchronous startup workflow.
Startup Flows	Select the Ellipsis (…) and specify the workflow to be run when the Workflow server starts.	These workflows are run in addition to Initial Startup Script. Workflows in this list are not guaranteed to execute in any particular order in relation to themselves, Initial Script, or arriving requests. Note that the Initial Script field also specifies a flow to be started, but that parameter can set only one flow. You can specify multiple Startup Scripts.
Semaphores	Select the Ellipsis (…) and specify the list of semaphores used by the workflows.	For more information about semaphores, see the *Avaya IC Media Workflow Reference*.
Directory tables	Select the Ellipsis (…) and specify the Directory server tables to be preloaded in memory at startup.	

Field	Recommended entry	Notes
Event Threads	Accept the default or enter a number of threads.	The default entry is 10. The number of threads that are listening and available to process events sent to the server.
Enable Heap Validate	Do not select this field unless: • You are instructed by Avaya Technical Support. • You are debugging a workflow.	This field is for debugging workflows only. Impacts performance of the Workflow server if selected. If the Workflow server fails when it runs a workflow, use this field to check each block as the workflow runs to ensure that the block does not corrupt the Heap.

6. Click **OK**.

Note:
Do not start this server before you configure all core servers. To ensure that the servers start correctly, see Starting and stopping IC servers on page 107.

Completing the Agent Prompting Workflow server configuration

For the Agent Prompting Workflow server, configure your agent desktop and your agents for Prompter and wrapup functionality. A sample Prompter workflow is included in the seed data.

This sample workflow is only intended to help you to test Prompter and agent wrapup. For information about how to create and modify Prompter workflows, see *Agent Script Workflow Reference*.

You complete the configuration of other Workflow servers when you configure the media channels and other components, such as the Unified Agent Directory, in your IC system. You do not need to configure these components at this point in your installation and configuration.

Creating a Blender server

The Blender server controls agent availability across the different channel types and monitors ADU change events.

The Blender server depends on the Workflow server. Therefore, you cannot configure the Blender server if you have not already performed the steps in Creating a Workflow server on page 94. If the Blender server connects to a Workflow server for a media channel, create the Blender server after you configure the Workflow server.

Do not assign a Blender server to a domain that cannot be reached by agents. If agents cannot reach the Blender server, the IC system will not operate correctly. The domain for a Blender server must meet **one** of the following guidelines:

- The Blender server must be in the same domain as a Workflow server and an ADU server.

  OR

- The failover path for the domain of the Blender server must include a Workflow server and an ADU server.

Important:
If the Blender server domain does not include a Workflow server and an ADU server, or those servers are not in the failover path for the Blender server, you will not be able to start the Blender server. For more information, see *Avaya IC Installation Planning and Prerequisites*.

The IC installation program automatically adds this server.

To create a Blender Server:

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **Blender**.
3. Click **OK**.
4. Click the **General** tab, and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	Blender_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Default` from the drop-down list if the server is in the Default domain.
Host	Select the IP address of the system from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. Click the **Blender** tab, and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
WorkFlow Server	Select the Workflow server used by this Blender server from the drop-down list.	If you only have one Workflow server and one Blender server, select Workflow_system. If your configuration includes multiple Workflow and Blender servers, select the Workflow server that you created to work with this Blender server.
Flow Set	Enter the name of the workflow project that contains the Blender flows.	The default name is blender.
Initialization Flow	Enter the name of the workflow that initializes the Blender server.	Default name is initialization.
Initialization Data Name	You can leave this field blank.	Optional field. The initialization data name contains values to be added to indata when InitRule is run. InitRule has an indata Event and outdata Event that fill in indata with a string (InitName) and seqcouple (InitData).
Initialization Data	You can leave this field blank.	Optional field. The name to add to indata when InitRule is run.
Client Login Flow	Enter the name of the Client Login workflow.	Default name is clientlogin.
Client Logout Flow	Enter the name of the Client Logout workflow.	Default name is clientlogout.

6. Click **OK**.

Note:
Do not start this server before you configure all core servers. To ensure that the servers start correctly, see Starting and stopping IC servers on page 107.

Creating an HTTP Connector server

The IC installer does not install the HTTP Connector server.

Prompters use the HTTP Connector server. You can create separate HTTP Connector servers for each of these features.

You can host more than one HTTP Connector server on a same system if the HTTP Connector servers use different HTTP ports.

To create an HTTP Connector server:

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **HTTPConnector** and click **OK**.
3. Click the **General** tab, and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	HTTPConnector_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Default` from the drop-down list if the server is in the Default domain.
Host	Select the IP address of the system from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Click the **HTTPConnector** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
IC Data Source	Select the application name associated with the server. This name should match the IC Data Source setting for the corresponding Workflow server.	If you used the default name, select `interaction_center`. You created this data source in Generating the Interaction Center application on page 151.
Workflow Server	Select the name or type of the Workflow server that this connector should use to execute Workflows and Prompter flows.	
Doc Directory	Accept the default or enter a new directory path.	The directory where the server looks for java script and error pages to serve to prompter and agent applications. Always consider as the relative path from the *`IC_INSTALL_DIR`*`\IC73\`.

Field	Recommended entry	Notes
Start Page	Accept the default or enter a new file name.	The name of the file that the Prompter serves when a client asks for a director.
Enable SSL	Select the check box if you want to enable the Secure Sockets Layer (SSL) security.	
Certificate File	The server certificate file that the HTTP Connector server uses.	The field is visible only when you select the Enable SSL check box.
Key File	The key file that the HTTP Connector server uses.	The field is visible only when you select the Enable SSL check box.
HTTP Port	Enter 9170 for default port.	The server uses this port for HTTP requests. If you must change this port, see *Avaya IC Installation Planning and Prerequisites* for a list of the default port numbers used by the other Avaya IC servers. Port conflicts can cause serious problems within the Avaya IC system. **Note:** If you run multiple HTTP Connector servers on the same system, ensure that they use different ports.
Request Timeout (sec)	Enter the number of seconds that the HTTP Connector should wait for a response from one of its clients.	The upper limit of the response time (in seconds) of the Workflow server. The HTTP Connector assumes the current HTTP request from the client has timed out if it did not receive a response from the Workflow server within this time interval. The default is 60 seconds.
Session Timeout (sec)	Enter the time in seconds that the agent has to complete a page and submit the information back to the server.	The maximum idle time for a session. Agent needs to complete and submit the information of the current page within the specified interval value. The HTTP Connector assumes the session as timed out if it does not receive any response from the agent within this time interval. The default is 600 seconds.

Field	Recommended entry	Notes
Request Handler Count	Enter the number of threads in the thread pool used by HTTP Connector server for processing VESP requests.	The default value is 50. The minimum value is 1.
Listener Thread Pool Size	Enter the number of threads in the thread pool used by HTTP Connector server for processing incoming TCP connections.	The default value is 50. The minimum value is 0 - in this case the thread pool will be disabled, and the number of threads used for processing incoming connections will not be limited (however, it may lead to resource consumption issues). This option is available since IC 7.3.11.

5. Click **OK**.
6. If the IC system includes support for:
   - Traditional Chinese, configure the language support as described in Configuring an HTTP Connector server for Traditional Chinese on page 514.
   - Russian, configure the language support as described in Configuring an HTTP Connector server for Russian on page 514.

Note:
Do not start this server before you configure all core servers. To ensure that the servers start correctly, see Starting and stopping IC servers on page 107.

Creating a Notification server

The IC installation program does not automatically add this server.

Before you create the Notification server, configure the SMTP and POP3 email servers and verify the configuration, as described in *Avaya IC Installation Planning and Prerequisites*.

To create a Notification server:

1. Select **Server** > **New** in IC Manager.
2. From the list of servers, select **Notification** and click **OK**.

3. Click the **General** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	Notification_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Default` from the drop-down list to add the server to that domain.
Host	Select the IP address of the system from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Click the **Notification** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
IC Data Source	Select the Interaction Center data source.	If you used the default name, select `interaction_center`. You created this data source in Generating the Interaction Center application on page 151.
Email Cluster	Select the Email Cluster name.	The primary email server of selected email cluster will be used to send email notification.
SMTP FQDN	Enter the fully qualified domain (FQDN) name of your Email server.	This is the Email server that Avaya IC uses for outbound email. For example, `MailSrvExchange.xyzcorp.com`. This field is no longer required in IC Release 7.3.3.
Default Sender Email Address	Enter a valid email address that acts as the sender of the notification emails.	For example, enter notify@xyzcorp.com. **Note:** Do not use an agent address as the Default Sender Email Address. This field is no longer required in IC Release 7.3.3.

Field	Recommended entry	Notes
Poll Interval (sec)	60	Number of seconds between polls.
Poll Future (sec)	86,400	Number of seconds for a long poll. The default equals 24 hours.
Search Limit	250	Number of database records for Notification Server to process at the same time.
Work Schedule Name	Enter the name of the work schedule, if required.	The name of the work schedule the server should use to determine business time.
Notification Agent	Accept the default, or enter another agent number, if required.	The number representing the agent for which this service instance responds. Agent #0 is the default, and catches all messages. You can also configure multiple Notification server agents, where Agent #1 is for all escalations and Agent #2 is for email and printer. **Note:** If you configure multiple Notification server agents, you cannot specify an Agent #0, because Agent #0 responds to all messages.
Fire Direct Notification	Select this field, if required.	Select this option if the server should fire notifications.
Fire Escalations	Select this field, if required.	Select this option if the server should send scheduled escalations.

Field	Recommended entry	Notes
Fire Scheduled Reports	Select this field, if required.	Select this option if the server should run scheduled reports.
Language	Select the language in which data for this server will be written.	The allowable codes are: • en (English) • fr (French) • de (German) • es (Spanish) • it (Italian) • pt (Portuguese) • zh (Chinese, Simplified) • ko (Korean) • ja (Japanese) • th (Thai) • zt (Traditional Chinese) • ru (Russian)

5. Click **OK**.
6. To configure an alternate email encoding for a language such as Japanese, see Configuring a Notification server for alternate email encodings on page 513.

Note:

Do not start this server before you configure all core servers. To ensure that the servers start correctly, see Starting and stopping IC servers on page 107.

Starting and stopping IC servers

After you add and configure the servers, you can modify the server configuration in IC Manager. However, if you modify multiple servers, you must start and stop the servers in a specific order. Dependencies between the servers determine the order. If you do not start and stop the servers in correct order, your IC system may lose data or encounter other problems. For more information, see *Interaction Center Administration Guide*.

CAUTION:
Never stop the DUStore server before you stop the EDU server. If you stop the DUStore server first, you may lose EDU data. Always stop these servers in the following order:

1. EDU server
2. ADU server
3. DUStore server
4. Report server

This section covers startup and shutdown for all IC servers, including some servers that you do not install and configure until later in the installation process.

This section includes the following topics:

- Determining server dependencies on page 107
- Starting and stopping the ORB server on page 110
- Starting and stopping servers in IC Manager on page 112
- Stopping all servers on page 112
- Starting and stopping servers with the IC Admin utility on page 112

Determining server dependencies

Starting and stopping servers in IC is a simple process. However, you should exercise caution because starting or stopping IC processes in the wrong order can lead to data loss or system errors. In addition, if your IC installation spans multiple systems, you need to pay attention to the order in which the systems are shut down because of the impact on other IC services.

This section includes the following topics:

- Server startup dependencies on page 108
- Server shutdown dependencies on page 109

Server startup dependencies

Servers can be started:

- Explicitly by an administrator.
- Automatically when the system, on which they reside, is started.
- As a result of a request from a client.

Tip:
The startup time for each server depends on factors, such as user population, number of queued emails, and database size. If your servers take a long time to start, you can reduce the server load by adjusting some of these dependencies.

To view the state of each server, use the **Server** tab and Alarm Monitor in IC Manager. As servers are started, that server's state changes to Up in the **Server** tab, and ORB server sends messages to the Alarm Monitor. If IC Manager is running and the Alarm server fails, IC prompts the administrator to immediately monitor alarms again.

The ICM, IC website (Tomcat), CIRS, and ICM Bridge (Attribute server) are dependent on several IC servers. These components perform a client login that, at minimum, requires the Directory, Alarm, ORB, and Data servers to be running.

To work with a Web Server such as IIS, IBM HTTP server, and Oracle iPlanet server, IC uses ISAPI and NSAPI filters respectively. These interfaces are used to enable Web Management, DataWake, and Tomcat support using plugins that can recover if a dependent component is not available.

The VOX server interfaces with an Interactive Voice Response (IVR) Unit. If the VOX server connects to an external IVR, you should start the IVR first. The VOX server attempts to connect to the configured IP address and port, for the length of time specified in the VOX server's Maximum Wait Time and Disable Wait parameters. If the IVR connects to the VOX server, the VOX server must be started first.

Tip:
For an IC deployment that includes IC and OA components on the same system, always start the IC components first, and then start the OA components to avoid potential port conflicts.

Server shutdown dependencies

Important:
Shutting down any IC server process or system may have an impact on agent clients and dependent processes. Therefore, you should only do so during non-business hours unless you are dealing with an emergency situation.

If failover is configured, the clients should revert from their primary to their backup servers. The connections to the backup server will remain active until the client logs out, is restarted, or another disruption in service occurs.

If failover is not configured and you stop an IC server, active clients may either raise alarms or show error dialogs and potentially fail if the server is down long enough.

If you need to shut down an IC server, you should:

- Do so during a scheduled maintenance period when clients are shut down and incoming activity can be restricted.
- Use the IC Manager Shutdown option to ensure the correct communication flow between IC components, IC clients, and the other services that should be stopped. The Shutdown option ensures that all IC server processes on that system are shut down in the correct order. It does not shut down dependent IC processes located on other system. To use this option, see Stopping all servers on page 112.

Before stopping the services on a system, you need to consider its impact. Other dependent clients, both agent clients and IC processes, may need to be shut down first.

To confirm that an IC process is shut down properly, use the System Administration tools provided with your operating system to ensure that the process is no longer active. IC Manager may report some servers as being stopped while they are actually finishing important clean up tasks such as committing data to the database.

IC processes should be restarted as soon as possible in order to minimize the impact on clients. In many cases, the processes restart automatically when the systems come back, or when client requests trigger the server to restart.

Dependent clients attempt to reconnect if they lose communication with an IC process. If the stopped process does not recover in time, request failover based on the server configuration and the failover strategy implemented at your site.

If you need to shutdown individual IC servers, follow the correct shutdown order to prevent data loss. Stopping a server results in disruption of the services provided by that server. The following table shows the impact of shutting down certain servers:

Server	Impact
Alarm server	This server is typically the last to be shutdown so that other servers can still submit alarms.
Data server	Without a Data server, other servers will be unable to commit, read, or write from the database.
DUStore server	If you have configured the ADU and EDU servers to persist data units, these servers become dependent on the DUStore server. Shutting down the DUStore server before the EDU or ADU servers will result in data units not being saved.
Event Collector server	Without the Event Collector, real time statistics will not be collected for the associated domain.
ORB server	This server is responsible for process management. If the ORB server is not running, no other IC server can start.

Starting and stopping the ORB server

The ORB server controls other IC servers. You must start the ORB server to open IC Manager. When you start the ORB server, the Alarm, Directory, EDU, and ADU servers start up in sequence.

CAUTION:
Do not stop ORB server using Windows Task Manager, or the Windows Services control panel.

The IC Configuration Tool starts the ORB server the first time. If you must stop and start the ORB server again, use the IC Admin utility or the IC Manager **Shutdown** option.

This section includes the following topics:

- ORB server components on page 111
- Configuring the ORB server to start automatically on Windows on page 111
- Configuring the ORB server to start automatically on Solaris or AIX on page 111

ORB server components

The following table describes the components of the ORB server:

Component	Description
orbsrv.exe	Executable for the ORB server.
qntorbsrv.exe	Windows service executable that starts the **orbsrv** executable.
IC ORB Service	Windows only. Helper service that represents the **qntorbsrv.exe** executable in the Windows Services control panel.

Configuring the ORB server to start automatically on Windows

The ORB server is set to automatically start when you install the server. However, if you reboot a system and the ORB server does not start, you can follow these steps to manually configure the ORB server.

To configure the ORB server to start automatically on a Windows system:

1. Select **Start** > **Control Panel** > **Services** to open the Windows Services control panel.
2. In the list of services, double-click **Avaya IC ORB Service 7.3**.
3. In the **General** tab, select **Automatic** from the **Startup Type** drop-down list.
4. Click **OK**.

Configuring the ORB server to start automatically on Solaris or AIX

To configure the ORB server to start automatically on the Solaris system:

1. Log in as root.
2. Navigate to the *IC_INSTALL_DIR*/IC73/bin directory.
3. Execute **setup_orb**.

Starting and stopping servers in IC Manager

IC Manager allows you to start multiple servers at the same time. The Status column displays the server's new status. If the system cannot start a server, IC Manager displays an error message.

CAUTION:
Never stop the DUStore server before you stop the EDU server. If you stop the DUStore server first, you may lose EDU data.

After you add and configure a server, stop and restart that server.

To start or stop a server:

1. In IC Manager, click the **Server** tab.
2. In the right pane, select a server that you want to stop.
3. Click the **Start server** or **Stop server** button on the toolbar.

Stopping all servers

You can simultaneously shut down all servers that reside on a system. The server shutdown feature in IC Manager shuts down the servers in the correct order. This process can take several minutes to complete as all servers must complete their current tasks before shutting down. For example, if there are a lot of persistent EDUs for email contacts, the DUStore server can take several minutes to write the EDUs to the database.

To shut down all servers:

1. In IC Manager, select **Server** > **Shutdown**.
2. Select the IP address or the name of the system where you want to shut down the servers.
3. Click **Ok**.

Starting and stopping servers with the IC Admin utility

You can use the IC Admin utility to:

- Start the ORB server and all IC servers that have Autostart enabled, as described in Starting servers with the IC Admin utility on page 113.
- Stop the ORB server and all associated IC servers, as described in Stopping all servers with the IC Admin utility on page 113.

For information about how to start and stop Web services, such as the ICM server, see Starting and stopping IC services on page 114,

Starting servers with the IC Admin utility

To start servers with the IC Admin utility:

1. Open the command prompt and go to the following directory:

Operating system	Directory
Windows	*IC_INSTALL_DIR*\IC73\bin
Solaris	*IC_INSTALL_DIR*/IC73/bin
AIX	*IC_INSTALL_DIR*/IC73/bin

2. Execute the following command:

   icadmin so

Stopping all servers with the IC Admin utility

To stop all servers on a system with the IC Admin utility:

1. Open the command prompt and go to the following directory:

Operating system	Directory
Windows	*IC_INSTALL_DIR*\IC73\bin
Solaris	*IC_INSTALL_DIR*/IC73/bin
AIX	*IC_INSTALL_DIR*/IC73/bin

2. Execute the following command:

   icadmin tv *<IC_administrative_user> <password>*

Accessing the help for the IC Admin utility

The IC Admin utility includes additional commands that are not listed in this section. The help for the IC Admin utility includes information about those additional commands.

To access the help for the IC Admin utility:

1. Open the command prompt and go to the following directory:

Operating system	Directory
Windows	*IC_INSTALL_DIR*\IC73\bin

Operating system	Directory
Solaris	*IC_INSTALL_DIR*/IC73/bin
AIX	*IC_INSTALL_DIR*/IC73/bin

2. Execute the following command:

   icadmin help

Starting and stopping IC services

When you use the **Web** tab of the Configuration Tool to configure Web applications, the Configuration Tool creates services for IC.

Tip:
You must configure all IC services to autostart.

This section describes how to stop, start, and configure startup options for the IC services, and how to set startup options for the services. This section includes the following topics:

- Starting and stopping services on Windows on page 114
- Starting and stopping services on Solaris on page 115
- Starting and stopping services on AIX on page 118

Starting and stopping services on Windows

Use the Windows Service Panel to start, stop, and configure startup options for IC services.

Note:
Depending upon the components installed on the system, not all of the following Windows services are displayed in the Windows Service Panel.

To start, stop and configure IC services on Windows:

1. In the Services control panel, right-click one or more of the following services:
   - Avaya IC 7.3 ICM Service
   - Avaya IC 7.3 CIRS Service
   - IC 7.3 SDK Service
   - IC 7.3 Web Services Service
   - World Wide Web Publishing Service (for IIS)

- Avaya IC Jakarta Service 7.3
- Avaya IC WebLM Service 7.3
- Avaya IC Web Management Service 7.3
- Avaya IC Email Template Management Service 7.3
- Avaya IC Test Service 7.3

2. From the right-click menu, select one of the options in the following table:

Task	Options
Start IC services	Select **Start**.
Stop IC services	Select **Stop**.
Set startup options	1. Select **Properties**. 2. Select **Automatic** from the **Startup Type** drop-down list. 3. Click **OK**.

Starting and stopping services on Solaris

This section includes the following topics:

- Starting and stopping the ICM server on page 115
- Starting and stopping the CIRS server on page 116
- Starting and stopping Oracle iPlanet Web server on page 116
- Starting and stopping Tomcat Web applications on page 116
- Setting Tomcat Web applications to autostart on page 117

Starting and stopping the ICM server

Execute all ICM server commands from the *IC_INSTALL_DIR*/IC73/bin directory. For the ICM server to be able to log in, the IC servers must start before the ICM server.

Starting the ICM server: To start the ICM server, execute the following command:

```
nohup ./icm.sh start
```

Stopping the ICM server: To stop the ICM server, execute the following command where -force is an optional parameter that terminates the server processes:

```
nohup ./icm.sh stop -force
```

Setting the ICM server to autostart: To set the ICM server to autostart, add the following command to the UNIX startup facility:

```
nohup bin/icm.sh start
```

Starting and stopping the CIRS server

Execute all CIRS server commands from the *IC_INSTALL_DIR*/IC73/bin directory. For the CIRS server to be able to log in, the IC servers must start before the CIRS server.

Starting the CIRS server: To start the CIRS server, execute the following command:

```
nohup ./cirs.sh start
```

Stopping the CIRS server: To stop the CIRS server, execute the following command where -force is an optional parameter that terminates the server processes:

```
nohup ./cirs.sh stop -force
```

Setting the CIRS server to autostart: To set the CIRS server to autostart, add the following command to the UNIX startup facility:

nohup *IC_INSTALL_DIR*/IC73/**bin/cirs.sh start**

Starting and stopping Oracle iPlanet Web server

Starting Oracle iPlanet Web Server: To start Oracle iPlanet Web Server, execute the following command:

```
<iplanet_home_dir>/https-instance_name/bin/startserv
```

Stopping Oracle iPlanet Server: To stop Oracle iPlanet Server, execute the stop script packaged with the Web server:

```
<iplanet_home_dir>/https-instance_name/bin/stopserv
```

Setting Oracle iPlanet Server to autostart: To set Oracle iPlanet server to autostart, add the following command to the UNIX startup script:

```
<iplanet_home_dir>/https-instance_name/bin/startserv
```

Starting and stopping Tomcat Web applications

Execute all Tomcat commands for the Web Applications from the *IC_INSTALL_DIR*/IC73/bin directory.

Starting all services on a system: To start services for all Web applications, execute the following command:

```
nohup ./ictomcat.sh start all
```

Stopping all services on a system: To stop all services for Web applications, execute the following command where `-force` is an optional parameter that terminates the server processes:

```
nohup ./ictomcat.sh stop all -force
```

Starting an individual Web application: To start an individual Web application, execute the appropriate command from the following table:

Web application	Start command
Website	**nohup ./ictomcat.sh start website**
csportal	**nohup ./ictomcat.sh start csportal**
Web License Manager	**nohup ./ictomcat.sh start weblm**
Email Template Administration	**nohup ./ictomcat.sh start rlmanager**
Client SDK server	**nohup ./ictomcat.sh start SDK**
Web Services server	**nohup ./ictomcat.sh start webservices**

Stopping an individual Web application: To stop an individual Web application, execute the appropriate command from the following table. `-force` is an optional parameter that terminates the server processes.

Web application	Stop command
Website	**nohup ictomcat.sh stop website -force**
csportal	**nohup ./ictomcat.sh stop csportal -force**
Web License Manager	**nohup ictomcat.sh stop weblm -force**
Email Template Administration	**nohup ictomcat.sh stop rlmanager -force**
Client SDK server	**nohup ./ictomcat.sh stop SDK -force**
Web Services server	**nohup ./ictomcat.sh stop webservices -force**

Setting Tomcat Web applications to autostart

To set Tomcat Web applications to autostart, add the following command to the UNIX startup facility:

nohup *IC_INSTALL_DIR*/IC73/**bin/ictomcat.sh start all**

For the Tomcat Web applications to be able to log in, the IC servers must start first.

Starting and stopping services on AIX

This section includes the following topics:

- Starting and stopping the ICM server on page 118
- Starting and stopping the CIRS server on page 118
- Starting and stopping IBM http Web server on page 119
- Starting and stopping Tomcat Web applications on page 119
- Setting Tomcat Web applications to autostart on page 120

Starting and stopping the ICM server

Execute all ICM server commands from the *IC_INSTALL_DIR*/IC73/bin directory. For the ICM server to be able to log in, the IC servers must start before the ICM server.

Starting the ICM server: To start the ICM server, execute the following command:

```
nohup ./icm.sh start
```

Stopping the ICM server: To stop the ICM server, execute the following command where -force is an optional parameter that terminates the server processes:

```
nohup ./icm.sh stop -force
```

Setting the ICM server to autostart: To set the ICM server to autostart, add the following command to the UNIX startup facility:

```
nohup bin/icm.sh start
```

Starting and stopping the CIRS server

Execute all CIRS server commands from the *IC_INSTALL_DIR*/IC73/bin directory. For the CIRS server to be able to log in, the IC servers must start before the CIRS server.

Starting the CIRS server: To start the CIRS server, execute the following command:

```
nohup ./cirs.sh start
```

Stopping the CIRS server: To stop the CIRS server, execute the following command where -force is an optional parameter that terminates the server processes:

```
nohup ./cirs.sh stop -force
```

Setting the CIRS server to autostart: To set the CIRS server to autostart, add the following command to the UNIX startup facility:

nohup *IC_INSTALL_DIR*/IC73/**bin/cirs.sh start**

Starting and stopping IBM http Web server

Execute the IBM http Web server commands from the *IC_INSTALL_DIR*/IC73/bin directory.

Starting IBM http Web Server: To start IBM http Web Server, execute the following command:

```
./httpserver.sh start
```

Stopping IBM http Web Server: To stop IBM http Web Server, execute the following command:

```
./httpserver.sh stop
```

Setting IBM http Web Server to autostart: To set IBM http Web server to autostart, add the appropriate command to the UNIX startup script. For example, add:

nohup *IC_INSTALL_DIR*/IC73/bin/httpserver.sh **start**

Starting and stopping Tomcat Web applications

Execute all Tomcat commands for the Web Applications from the *IC_INSTALL_DIR*/IC73/bin directory.

Starting all services on a system: To start services for all Web applications, execute the following command:

```
nohup ./ictomcat.sh start all
```

Stopping all services on a system: To stop all services for Web applications, execute the following command where -force is an optional parameter that terminates the server processes:

```
nohup ./ictomcat.sh stop all -force
```

Starting an individual Web application: To start an individual Web application, execute the appropriate command from the following table:

Web application	Start command
Website	**nohup ./ictomcat.sh start website**
Web License Manager	**nohup ./ictomcat.sh start weblm**
Email Template Administration	**nohup ./ictomcat.sh start rlmanager**
Client SDK server	**nohup ./ictomcat.sh start SDK**
Web Services server	**nohup ./ictomcat.sh start webservices**

Stopping an individual Web application: To stop an individual Web application, execute the appropriate command from the following table. `-force` is an optional parameter that terminates the server processes.

Web application	Stop command
Website	**nohup ictomcat.sh stop website -force**
Web License Manager	**nohup ictomcat.sh stop weblm -force**
Email Template Administration	**nohup ictomcat.sh stop rlmanager -force**
Client SDK server	**nohup ./ictomcat.sh stop SDK -force**
Web Services server	**nohup ./ictomcat.sh stop webservices -force**

Setting Tomcat Web applications to autostart

To set them to autostart, add the following command to the UNIX startup facility:

nohup *IC_INSTALL_DIR*/IC73/**bin/ictomcat.sh start all**

For the Tomcat Web applications to be able to log in, the IC servers must start first.

Chapter 6: Configuring databases

This section describes how to configure the IC data server, databases, and data sources. All IC systems require an IC Repository database and a CallCenterQ database.

This section includes the following topics. Perform the steps in the order set below.

1. Before you configure IC databases on page 122
2. Copying the stored procedure library - DB2 only on page 123
3. Setting up a Data server on page 123
4. IC data sources on page 132
5. Setting the display time for IC databases on page 133
6. Creating IC Repository on page 134
7. Creating the CCQ database on page 143

Before you configure IC databases

Before you configure the IC databases, complete the following prerequisites:

Install IC servers: You must create and configure the primary server environment and then start the primary servers before you can configure the IC servers and components.

You must do the following:

- On a system that hosts the IC primary ORB server, install the IC server files and configure the primary server environment.
- On a system that hosts the Data server, install the IC server files and configure the server environment. If this system is different from the one that hosts the primary ORB server, configure a secondary server environment on this system.

If you have not installed the server files, see Installing IC server components on page 35.

Install IC Design and Administration tools: Install these tools on a dedicated system that has network access to all server systems. For information on how to install these tools, see Installing IC server components on page 35.

Install database management system: For more information, see *Avaya IC Installation Planning and Prerequisites* and the documentation provided with the database management system.

Install and configure the database client software: The database client software also includes the vendor libraries, and support files. Install and configure these files on a system that hosts the Data server. The Data server requires the database client software to communicate with the database. For example, if your IC system includes a supported Oracle database, install the Oracle client for that version on a system that hosts the Data server.

Database connections: Configure and validate the database software connections on a system where you plan to install the Data server.

Copying the stored procedure library - DB2 only

If you host your IC databases on DB2, you must copy the `qdb2sp` stored procedure library from the system that hosts the primary ORB server to the system that hosts the IC database instance.

To copy the `qdb2sp` stored procedure library to the DB2 server installation hierarchy:

1. On a system that hosts the DB2 Data server, navigate to the *`IC_INSTALL_DIR`*`/IC73/lib` directory where IC installs the `qdb2sp` stored procedure library.
2. Use the **`ftp`** command or the **`rcp`** command to copy the `qdb2sp` stored procedure library to the **`db2inst1/sqllib/function`** directory on a system that hosts the DB2 server:

Note:
Do not copy the stored procedure library to any system that hosts the DB2 client. The stored procedure library must be copied to the function directory of the DB2 server.

Setting up a Data server

The Data server is specific to the type of database you use in your IC system. All IC server and client components use the Data server to communicate with your database. The Data server uses the IC account for each component or user to link the IC components and the database server.

All Data servers support connection pooling.

After you configure the Data server, you can configure other IC applications on the same system.

This section includes the following topics:

- Cautions and tips for configuring a Data server on page 124
- Creating the primary Data server on page 124

- Creating a secondary Data server on page 132

Cautions and tips for configuring a Data server

When you configure the Data server, note the following:

Database system: Do not install and configure the Data server on a system that hosts your database.

Host your database server on a dedicated system, so you can tune your database server to maximize database operations and improve the reliability and performance of the database.

Multiple database types: A Data server can only communicate with one type of database. Install multiple Data servers if your IC configuration requires more than one type of database. For example, you need a second Data server if you maintain a legacy database in a different type of database.

The CCQ database, IC Repository database, and OA database must all be of the same database type.

DB2 stored procedure library: If you use DB2 for your IC databases, you must copy the `qdb2sp` stored procedure library from the system that hosts the primary ORB server to the DB2 installation hierarchy. If you do not copy the stored procedure library, the Data server will not be able to communicate with the DB2 database server, and Database Designer will not be able to configure the IC databases. For more information, see Copying the stored procedure library - DB2 only on page 123.

Creating the primary Data server

The primary Data server is typically on the same system as the primary ORB server.

This section includes the following topics:

- Creating a primary Data server for Microsoft SQL Server on page 124.
- Creating a primary Data server for Oracle on page 127.
- Creating a primary Data server for IBM DB2 on page 130.

Creating a primary Data server for Microsoft SQL Server

To create a primary Data server for Microsoft SQL Server:

1. On a system where you installed the Design & Administration Tools, select **Start** > **Programs** > **Avaya Interaction Center 7.3** > **IC Manager**.

2. Log in to IC Manager with the pre-assigned login ID and password shown in the following table:

Login	Password
Admin	admin

   The next time you log in, IC Manager prompts you to change the password.

3. Click the **Server** tab, and:
   a. Select **Server** > **New**.
   b. From the list of servers, select **DataServerMSSQL**.
   c. Click **Ok**.
4. On the **General** tab of the Server Editor, enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	Enter a logical name for the Data server. For example, DataServerMSSQL.	Include the type of database on your IC system in the name. You need this name to configure Avaya IC Repository and the CCQ database.
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Default` from the drop-down list if the server is in the Default domain.
Host	Select the IP address of the system that hosts the server, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. On the **DataServer** tab of the Server Editor, enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
DB Login	Enter your DBA user name.	The name used by the Data server to access databases.
DB Password	Enter your database password.	The password that corresponds to the database login name used by the Data server to access databases.

Field	Recommended entry	Notes
SQL Driver (Windows Only)	Select an appropriate ODBC driver.	The drop-down list displays only the ODBC drivers that you installed on the system. **Note**: This field is available only for IC 7.3.3 and later. For example: • SQL Server (Installed with Windows OS) • SQL Server Native Client 10.0 (Installed with SQL Server 2008) • SQL Server Native Client 11.0 (Installed with SQL Server 2012) **Note:** If you enter value for ODBC driver in DB designer and in the DataServer's configuration, the DataServer ODBC information overrides the value provided by the DB designer. **Note**: If you are configuring multiple Poller clusters with separate data servers for each Poller server, then with high load of incoming email contacts, database table lock issue might occur with SQL server Native client 10 and 11. If such a situation occurs, Avaya recommends the use of only "SQL Server" old client for data server configuration.

Field	Recommended entry	Notes
Request Handler Thread Pool Size	Enter the number of requests in the thread pool. The default value is 30.	Maximum number of threads that handle client requests in the Data server. These threads accept requests from the Data server clients and queues them for execution in the database.
DB Connection Pool Size	Enter the number of connections in the pool. Default is 15. Minimum is 1.	Maximum number of database connections to open in a connection pool.

6. Click the **Debug** tab and perform the following steps:
   a. Click the **Ellipsis** (**…**) button next to **Trace Levels**.
   b. In the **Trace Levels** dialog box, select the following check boxes.

Field	Recommended entry	Notes
idl	• Select this box for development systems only. • Clear this box for production systems.	idl is a higher level trace that is more readable than msg. idl writes all method invocations to the log file.
flush	• Select this box for development systems only. • Clear this box for production systems.	When the server writes to the log buffer, flush immediately writes the information to the log file. Flush does not wait for the buffer to fill before writing entries to the log file.

   c. Click **OK**.

   For information about the other options in the **Trace Levels** dialog box, see *Interaction Center Administration Guide*.
7. Click **OK** to save the Data server configuration.
8. Right-click the Data server that you have created and select **Start**.

Creating a primary Data server for Oracle

To create a primary Data server for Oracle:

1. On a system where you installed the Design & Administration Tools, select **Start** > **Programs** > **Avaya Interaction Center 7.3** > **IC Manager**.

2. Log in to IC Manager with the pre-assigned login ID and password shown in the following table:

Login	Password
Admin	admin

   The next time you log in, IC Manager prompts you to change the password.

3. Click the **Server** tab, then:
   a. Select **Server** > **New**.
   b. From the list of servers, select **DataServerOracle**.
   c. Click **Ok**.

4. In the **General** tab of the Server Editor, enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	Type DataServerOracle or another logical name for the Data server.	Include the type of database on your IC system in the name. You need this name to configure Avaya IC Repository and the CCQ database.
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Default` from the drop-down list if the server is in the Default domain.
Host	Select the IP address of the system that hosts the server, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. On the **DataServer** tab of the Server Editor, enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
DB Login	Enter the database account name.	The database login name used by the Data server to access databases.
DB Password	Enter the password for the database account.	The password as configured in the Oracle database.

Field	Recommended entry	Notes
Oracle Home Directory	Enter the pathname of the home directory of the Oracle database.	Oracle Data server only. This home directory overrides the home directory specified in the Avaya IC Data Source parameter.
Request Handler Thread Pool Size	Enter the number of requests in the thread pool. Default is 30.	Maximum number of threads that handle client requests in the Data server. These threads accept requests from the Data server clients and queues them for execution in the database.
DB Connection Pool Size	Enter the number of connections in the pool. Default is 15. Minimum is 1.	Maximum number of database connections to open in a connection pool.

6. Click the **Debug** tab and perform the following steps:
   a. Click the **Ellipsis** (**…**) button next to **Trace Levels**.
   b. In the **Trace Levels** dialog box, select the following check boxes:

Field	Recommended entry	Notes
idl	• Select this box for development systems only. • Clear this box for production systems.	idl is a higher level trace that is more readable than msg. idl writes all method invocations to the log file.
flush	• Select this box for development systems only. • Clear this box for production systems.	When the server writes to the log buffer, flush immediately writes the information to the log file. Flush does not wait for the buffer to fill before writing entries to the log file.

   c. Click **OK**.

   For information about the other options in the **Trace Levels** dialog box, see *Interaction Center Administration Guide*.
7. Click **OK** to save the Data server configuration.
8. Start the Data server.
   a. Right-click the Data server that you have created and select **Start**.

Creating a primary Data server for IBM DB2

To create a primary Data server for IBM DB2:

1. On a system where you installed the Design & Administration Tools, select **Start** > **Programs** > **Avaya Interaction Center 7.3** > **IC Manager**.
2. Log in to IC Manager with the pre-assigned login ID and password shown in the following table:

Login	Password
Admin	admin

   The next time you log in, IC Manager prompts you to change the password.
3. Click the **Server** tab, then:
   a. Select **Server** > **New**.
   b. From the list of servers, select **DataServerDB2**.
   c. Click **Ok**.
4. On the **General** tab of the Server Editor, enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	Type DataServerDB2 or another logical name for the Data server.	Include the type of database on your IC system in the name. You need this name to configure Avaya IC Repository and the CCQ database.
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Default` from the drop-down list if the server is in the Default domain.
Host	Select the IP address of the system that hosts the server, or type in the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. On the **DataServer** tab of the Server Editor, enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
DB Login	Enter your database login name.	The name used by the Data server to access databases.
DB Password	Enter your database password.	The password that corresponds to the database login name used by the Data server to access databases.
Request Handler Thread Pool Size	Enter the number of requests in the thread pool. Default is 30.	Maximum number of threads that handle client requests in the Data server. These threads accept requests from the Data server clients and queues them for execution in the database.
DB Connection Pool Size	Enter the number of connections in the pool. Default is 15. Minimum is 1.	Maximum number of database connections to open in a connection pool.

6. Click the **Debug** tab and perform the following steps:
   a. Click the **Ellipsis** (**…**) button next to **Trace Levels**.
   b. In the **Trace Levels** dialog box, select the following check boxes.

Field	Recommended entry	Notes
idl	• Select this box for development systems only. • Clear this box for production systems.	idl is a higher level trace that is more readable than msg. idl writes all method invocations to the log file.
flush	• Select this box for development systems only. • Clear this box for production systems.	When the server writes to the log buffer, flush immediately writes the information to the log file. Flush does not wait for the buffer to fill before writing entries to the log file.

   c. Click **OK**.

   For more information about trace levels, see *Interaction Center Administration Guide*.
7. Click **Ok**.
8. Start the Data server:

a. Right-click the Data server that you have created and select **Start**.

Creating a secondary Data server

An IC system usually requires more than one Data server. For information about recommended deployments for a secondary Data server, see *Avaya IC Installation Planning and Prerequisites*.

To create a secondary Data server, follow the instructions in Creating the primary Data server on page 124.

IC data sources

Application Design Language (ADL) files contain the data models for IC databases, including tables, table sets, browsers, and modules.

For an out-of-the-box, non-customized IC installation, use ADL files to perform the following tasks:

- Configure IC databases
- Create IC data sources

About data sources

All IC components that must access a database use IC data sources. These components include servers, workflows, and agent applications. You can create an IC data source when you generate an application from the application ADL file.

All IC systems require the following data sources:

- Repository data source
- Interaction Center data source

Repository and Interaction Center are only data sources that do not have a user interface. Although you can generate a Windows application to create the data sources, you cannot use repository or interaction_center as an application.

CAUTION:
Ensure that you select the appropriate data source for each server. Otherwise, the servers might become nonfunctional.

The following table describes the typical data sources in an out-of-the-box IC installation:

Data Source	ADL File	Description
repository	repository.adl	**Required for all Avaya IC systems.** Used by the Directory server, Report server, and DUStore server for access to the IC Repository.
interaction_center	ccq.adl	**Required for all Avaya IC systems.** Used by most IC servers to access the database. This data source also handles most server-related transactions, such as workflows. **Note:** Use this data source for all IC systems that integrate with third party applications.

Setting the display time for IC databases

When you create an IC database, you must set the display time for that database. The display time option determines how Avaya IC handles the difference in time between the agent desktop system and the time as reported by the database for all database activities, such as Select, Insert, and Update.

The following table describes the display time options for IC databases:

Display time option	Description
DBMSTIME	Select this option if you want the DateTime data to display as database time, and not adjusted to local time. With DBMSTIME, IC ignores the difference in time and does not apply the difference to any database activity.

Display time option	Description
LOCALTIME	Select this option if you want the DateTime data to display as adjusted to local time on the client. With LOCALTIME, IC uses the difference in time, rounds it to the nearest half hour, and applies this difference to all database activity that involves date and time information.
HOSTTIME	Select this option if you want the DateTime data to display as adjusted to the local host time, including small differences between system clocks. With HOSTTIME, IC uses the difference in time and applies this difference to all database activity that involves date and time information.

Creating IC Repository

IC Repository manages current and historical data in the form of Electronic Data Units (EDUs), Agent Data Units (ADUs), system configuration, and resource utilization statistics. The data includes agents, workgroups, queues, and tenants. IC Repository forms the structure that your database server needs to accept contact data from the IC EDU server and ADU server.

OA queries the data that these IC components write in the IC Repository database and other IC databases. OA then reports on the results of the queries.

To create IC Repository, complete the steps in the following topics:

1. Before you create IC Repository on page 134
2. Building the IC Repository database on page 135
3. Generating the IC Repository application on page 142
4. Updating the Directory server with IC Repository on page 142

Before you create IC Repository

Before you build the IC Repository database:

- You must know the names that you will give to your IC Repository and CCQ databases.
- For a localized version of IC, enable Localization in Database Designer, as described in Enabling Database Designer for localization on page 505.

Building the IC Repository database

The following instructions assume that you have reviewed and modified all components of the IC Repository ADL file in Database Designer. For information about the ADL file, see *IC Database Designer Application Reference*.

Important:
If you use DB2 for your IC databases, you must copy the qdb2sp stored procedure library from the system that hosts the primary ORB server to the DB2 installation hierarchy. For more information, see Copying the stored procedure library - DB2 only on page 123.

To build the IC Repository database, perform the steps in the following topics:

1. Configuring the IC Repository database connection on page 135
2. Configuring the IC Repository connection set on page 139
3. Creating the IC Repository database on page 140

Configuring the IC Repository database connection

To configure the IC Repository database connection:

1. In Database Designer, select **File** > **Open**.
2. Open the IC Repository ADL file.

   The ADL file is in *IC_INSTALL_DIR*\IC73\design\repository\repository.adl

   If you enabled Database Designer for localization, click **OK** and ignore the warning. Database Designer automatically generates the ALF file when you save the ADL file. For more information, see Enabling Database Designer for localization on page 505.
3. In the tree pane, expand **Components** > **Physical DB Connections** and select **repositoryDBConnection**.
4. In the DB Connection **Properties** tab, enter the information for the fields in the General group mentioned in the following table:

Property	Recommended entry	Notes
Timeout (sec)	Type the maximum number of seconds that the client application waits for a response to a database request before the application assumes the connection to the Data server is lost.	Default value is 60 seconds. If no response is returned within the specified time, the client application closes the connection to the Data server and returns an error. The client application attempts to create a new connection to the database on the next database request.

Property	Recommended entry	Notes
Description	Type a description of the database connection, if required.	You can leave this field empty.
Display Time	Select a display time option.	The display time option determines how IC handles the difference in time between the agent desktop system and the time as reported by the Database for all database activities, such as select, insert, and update. For more information about the display time options, see Setting the display time for IC databases on page 133.

5. From the **Database Type** drop-down list, select the type of database to which you want to connect.

   Database Designer uses the selected database type to generate a SQL statement which can be applied to the database.

6. Enter the information for the mandatory fields for your database mentioned in the following table:

Database type	Property	Recommended entry	Notes
All database types	Data Server Type	Type the name of the primary Data server.	This server is the one that you created in Setting up a Data server on page 123. For example, the default values are: • DataServerMSSQL • DataServerOracle • DataServerDB2
SQL Server	Database server	Type the host name of the system that hosts your database server.	For the default database instance, type the host name. For another database instance, type <*system*>\<*db_name*>
	Database Name	Type the name of the IC Repository database. For example, **`repository`**.	Use **`repository`** to reduce the possibility of a migration impact.

Database type	Property	Recommended entry	Notes
Oracle	TNS Name	Type the server alias from the tnsnames.ora file	For example, type support.xyzcorp.com.
	Database Name	Type the name of the Oracle user for the IC Repository database. For example, **repository**.	Use the **repository** to reduce the possibility of a migration impact.
	Client Library Home Directory	Type the full directory path for the Oracle client on the system that hosts the Data server.	For example, type `...\opt\oracle\Ora11`
DB2	DB2 Database Name	Type the name of the DB2 database that includes the IC schema.	DB2 allows a maximum of eight characters for database names. For example, type `db2IC`.
	Avaya IC Schema Name	Type the schema name of the IC Repository database. For example, **repository**.	Use the **repository** to reduce the possibility of a migration impact.
	Database Territory	Type the territory that represents the locale of the database that includes the IC Repository schema.	The territory defines the language and locale of the database. For more information, see the DB2 documentation.

7. Enter information for the optional fields for your database mentioned in the following table:

Database type	Property	Recommended entry	Notes
SQL Server	Database Location	Leave this field blank.	Identifies the logical space where the named database is stored. The SQL Server DBMS specifies the database location.
	Database Size	Leave this field blank.	The size of the database location specifies the amount of space that the configured application database occupies. The SQL Server RDBMS specifies the database size.
	Log Location	Leave this field blank.	Database-generated log files store cumulative transaction information. The SQL Server RDBMS specifies a default location for the database log.
	Log Size	Leave this field blank.	The size of the location for database log files specifies the amount of space that the database-generated log files can occupy. The SQL Server RDBMS specifies a default size for the database log.

Database type	Property	Recommended entry	Notes
Oracle	Default tablespace name	Type the name of the default tablespace where objects are created for the IC databases. For example, type **T_CI**.	The database location identifies the logical space where the named database is stored. If you leave this field blank, and the Oracle RDBMS does not specify a database location, Oracle uses the “system” space to define the database. **Caution:** Configuring a database in the system space can crash your database.
	Default tablespace size	Type the number of bytes for the size of the default tablespace.	**Caution:** If you do not specify a default tablespace size here, and your RDBMS does not define the default tablespace size, the default tablespace can expand to use all available space.
	Temp tablespace name	Type the name of the tablespace that stores temporary files. For example, type **T_CI_TEMP**.	Temporary tables store database-generated intermediate sorting files and client session information for Oracle databases. If you do not specify a location for temporary tables, the location is specified by the Oracle RDBMS.
DB2	Catalogued Node	Type the remote node on the system that hosts the Data server.	Complete this field if you host your Data server on a different system from the IC databases.
	Tablespace Name	Type the name of the tablespace used by the IC Repository database.	Complete this field if you created a dedicated tablespace that the IC Repository database uses. **Note:** OA requires dedicated tablespaces. For more information, see *Avaya OA Installation Planning and Prerequisites*.

8. Select **File** > **Save** to save the ADL file. Do not close the file.

Configuring the IC Repository connection set

To configure the connection set for IC Repository:

1. In the tree pane of Database Designer, expand **DB Connection Sets** and select **DefaultDBConnectionSet**.

2. On the **Connection Set Properties** tab, select **Application** from the **Logical DB Connections** list.
3. Make sure the properties are set as shown in the following table:

Field	Recommended entry
Physical DB Connection	Select **repositoryDBConnection**.
Primary	Do not check this box.
Use External Database	Check this box.
Database Name	Type the name of your application database. This name must be the exact name that you will give your application database when you create it. For example, type **ccq**.

4. From the **Logical DB Connections** list, select **Repository**.
5. Make sure the properties are set as shown in the following table:

Field	Recommended entry
Physical DB Connection	Select **repositoryDBConnection**.
Primary	Check this box.

6. Select **File** > **Save** to save the ADL file. Do not close the file.

Creating the IC Repository database

Creating Avaya IC repository database perform the following:

- Create the schema that IC requires for IC Repository.
- Seed IC Repository with the configuration data in the `seed.cfg` file.

You do not need to modify the IC Repository seed data. The following table describes the contents of the seed data for IC Repository:

Type of data	Description
Property data	System configuration data for IC Manager and Avaya Agent.

Type of data	Description
Initialization data	Default workgroup, queue, and tenant data for Web Management and Email Management. This data also includes templates you can use to create custom workgroups, queues, and tenants.
Mapping data	Default mapping rules for the Report Server. These rules tell the server how to write data from retired EDUs to IC Repository.

To create the IC Repository database:

1. In Database Designer, select **File** > **Database Administration**.
2. From the **DB Connection Set** list, select **defaultDBConnectionSet**.
3. Set the options as shown in the following table:

Field	Database type	Recommended entry
Configure	SQL Server	Select **Configure**.
	Oracle	Select **Configure**.
	DB2	Select one of the following options: • If you have run the `db2crdb.sh` script to create the database, *or* if you have already configured an IC database, select **Schema Only**. • If you have not run the `db2crdb.sh` script *and* if you have not yet configured an IC database, keep **Schema Only** unchecked and select **Configure**.
Import Seed Data	All database types	Check this box.
Login Id	All database types	Type your IC Manager login ID. **Note:** Do not use your DBA login ID and password.
Password	All database types	Type your password.

4. Click **Run** to configure the database and import the seed data.

   Database Designer pauses briefly between configuring the database and importing the seed data.
5. Click **Close** to close the Database Administration screen. Do not close the ADL file.

Generating the IC Repository application

You generate the IC Repository application to initialize the database with the ADL and version information, and to create the Repository data source.

To generate the IC Repository application

1. In Database Designer, select **File** > **Generate Windows Application**.
2. Check the following boxes to load the files to the database:
   - Messages
   - Avaya IC Scripts
3. From the **Name** list, select **repository**.
4. Type the path for the directory where you want Database Designer to store the application files.

   For example, type `AVAYA_IC73_HOME\apps`.

   If you do not know the directory path, click the **Ellipsis** (**…**) button and navigate to the directory.
5. From the **DB Connection Set** drop-down list, select **defaultDBConnectionSet**.
6. If the fields in the following table do not have entries, re-type your IC Manager account and password:

Field	Recommended entry
Login Id	Type your IC Manager login ID. **Note:** Do not use your DBA login ID and password.
Password	Type your password.

7. Click **OK**.

   Database Designer creates a new folder with the same name as the application in the target directory.

Updating the Directory server with IC Repository

You must initialize the connection between the Directory server and IC Repository. Until this point in the configuration, your IC ORB environment obtained configuration information from the local hard drive of the system. After you update the Directory server, the IC ORB environment obtains and stores configuration information in IC Repository.

To update the Directory server for IC Repository:

1. On the **Server** tab in IC Manager, double-click **Directory server**.
2. Click the **Directory** tab.
3. Verify that the IC Repository data source is selected from the **IC Data Source** drop-down list.
4. Click **OK**.
5. Stop and start the Directory server.

   The Alarm Monitor should display a message such as "Server has started: DS" followed by the IP address of the system that hosts the Directory server, the port used to communicate with the server, and an identification string.
6. When the Alarm Monitor indicates that the Directory server started properly, refresh IC Manager:
   a. Select **Manager** > **Refresh**.
   b. In the Success message, click **OK**.

   If you do not receive a Success message, perform the steps in Troubleshooting the refresh in IC Manager on page 499.

Note:
If you prefer to create and configure all databases at the same time, you can also create and configure the other databases used by your IC system at this time. For the OA databases, see the *Operational Analyst Installation and Configuration*.

Creating the CCQ database

You must create and seed the CCQ database to run all IC components and applications.

The CCQ database collects, stores, and manages:

- Customer-specific data, including contact information and customer history information.
- Application data, including information about Web Management or Email Management.

Note:
If you use DB2 for your IC databases, you must copy the `qdb2sp` stored procedure library from the system that hosts the primary ORB server to the DB2 installation hierarchy. If you do not copy the stored procedure library, Database Designer will not be able to configure the IC databases. For more information, see Copying the stored procedure library - DB2 only on page 123.

To create the CCQ database, complete the steps in the following topics:

1. Modifying the Avaya Agent layout on page 144.
2. Building the CCQ database on page 144.
3. Generating the Interaction Center application on page 151.

Modifying the Avaya Agent layout

If your system does not include Avaya Agent, do not perform this step. Go to Building the CCQ database on page 144.

IC installs the default Avaya Agent layout in the following directory:

IC_INSTALL_DIR\IC73\design\QConsole\avaya_agent_<lang>.cdl

where ***<lang>*** represents the language that the agent will use on the desktop. For example, if the agent desktop includes Avaya Agent in English, select `avaya_agent_en.cdl`. For more information about Avaya Agent layouts in non-English languages, see Configuring Avaya Agent for a supported language on page 507.

The default layout includes task lists for all media channels, including Telephony, Web Management, and Email Management. To customize the Avaya Agent layout for your contact center, see *Avaya Agent Integrator's Guide*.

Building the CCQ database

To build the CCQ database, perform the steps in the following topics:

1. Configuring the CCQ database connection on page 144
2. Configuring the CCQ connection set on page 150
3. Creating the CCQ database on page 150

Configuring the CCQ database connection

To configure the CCQ database connection:

1. If you do not already have the CallCenterQ ADL file open in Database Designer, select **File** > **Open**.

   You can find this ADL file in *IC_INSTALL_DIR*\IC73\design\CallCenterQ\ccq.adl

2. In the tree pane, expand **Components** > **Physical DB Connections** and select **ccqDBConnection**.

3. In the DB Connection **Properties** tab, enter the information for the fields in the General group mentioned in the following table:

Property	Recommended entry	Notes
Timeout (sec)	Type the maximum number of seconds that the client application waits for a response to a database request before the application assumes the connection to the Data server is lost.	Default value is 60 seconds. If no response is returned within the specified time, the client application closes the connection to the Data server and returns an error. The client application attempts to create a new connection to the database on the next database request.
Description	Type a description of the database connection, if required.	You can leave this field empty.
Display Time	Select a display time option.	The display time option determines how IC handles the difference in time between the agent desktop system and the time as reported by the Database for all database activities, such as select, insert, and update. For more information about the display time options, see Setting the display time for IC databases on page 133.

4. From the **Database Type** drop-down list, select the type of database to which you want to connect.

   Database Designer uses the selected database type to generate a SQL statement which can be applied to the database.

5. Enter the information for the mandatory fields for your database mentioned in the following table:

Database type	Property	Recommended entry	Notes
All database types	Data Server Type	Type the name of the primary Data server.	This server is the one that you created in Setting up a Data server on page 123. For example, defaults are: • DataServerMSSQL • DataServerOracle • DataServerDB2
SQL Server	Database server	Type the host name of the system that hosts your database server.	For the default database instance, type the host name. For another database instance, type <*system*>\<*db_name*>.
	Database Name	Type the name of the CallCenterQ database. For example, **ccq**.	Use the **ccq** to reduce the possibility of a migration impact.
Oracle	TNS Name	Type the server alias from the tnsnames.ora file	For example, type support.xyzcorp.com.
	Database Name	Type the name of Oracle user for the CallCenterQ database. For example, **ccq**.	Use the **ccq** to reduce the possibility of a migration impact.
	Client Library Home Directory	Type the full directory path for the Oracle client on the system that hosts the Data server.	For example, type `.../opt/oracle/Ora11`

Database type	Property	Recommended entry	Notes
DB2	DB2 Database Name	Type the name of the DB2 database that includes the IC schema.	DB2 allows a maximum of eight characters for database names. For example, type `db2IC`.
	Avaya IC Schema Name	Type the schema name of the CallCenterQ database. For example, **ccq**.	Use the **ccq** to reduce the possibility of a migration impact.
	Database Territory	Type the territory that represents the locale of the database that includes the CallCenterQ schema.	The territory defines the language and locale of the database. For more information, see the DB2 documentation.

6. If necessary, enter the information for the optional fields for your database mentioned in the following table:

Database type	Property	Recommended entry	Notes
SQL Server	Database Location	Leave this field blank.	Identifies the logical space where the named database is stored. The SQL Server DBMS specifies the database location.
	Database Size	Leave this field blank.	The size of the database location specifies the amount of space that the configured application database occupies. The SQL Server RDBMS specifies the database size.
	Log Location	Leave this field blank.	Database-generated log files store cumulative transaction information. The SQL Server RDBMS specifies a default location for the database log.
	Log Size	Leave this field blank.	The size of the location for database log files specifies the amount of space that the database-generated log files can occupy. The SQL Server RDBMS specifies a default size for the database log.

Database type	Property	Recommended entry	Notes
Oracle	Default tablespace name	Type the name of the default tablespace where objects are created for the IC databases. For example, type **T_CCQ**.	The database location identifies the logical space where the named database is stored. If you leave this field blank, and the Oracle RDBMS does not specify a database location, Oracle uses the “system” space to define the database. **Caution:** Configuring a database in the system space can crash your database.
	Default tablespace size	Type the number of bytes for the size of the default tablespace.	**Caution:** If you do not specify a default tablespace size here, and your RDBMS does not define the default tablespace size, the default tablespace can expand to use all available space.
	Temp tablespace name	Type the name of the tablespace that stores temporary files. For example, type **T_CCQ_TEMP**.	Temporary tables store database-generated intermediate sorting files and client session information for Oracle databases. If you do not specify a location for temporary tables, the location is specified by the Oracle RDBMS.
DB2	Catalogued Node	Type the remote node on the system that hosts the Data server.	Complete this field if you host your Data server on a different system from the IC databases.
	Tablespace Name	Type the name of the tablespace used by the CallCenterQ database.	Complete this field if you created a dedicated tablespace that the IC Repository database uses. **Note:** OA requires dedicated tablespaces. For more information, see *Avaya OA Installation Planning and Prerequisites*.

7. Select **File** > **Save** to save the ADL file. Do not close the file.

Configuring the CCQ connection set

To configure the CCQ connection set:

1. In the tree pane of Database Designer, expand **DB Connection Sets** and select **DefaultDBConnectionSet**.
2. Click the **Connection Set Properties** tab.
3. From the **Logical DB Connections** list, select **CallCenterQ** and make sure that the properties are set as shown in the following table:

Field	Recommended entry
Physical DB Connection	Select **ccqDBConnection**.
Primary	Check this box.

4. Select **Repository** from the **Logical DB Connections** list and make sure the properties are set as shown in the following table:

Field	Recommended entry
Physical DB Connection	Select **ccqDBConnection**.
Primary	Do not check this box.
Use External Database	Check this box.
Database Name	Type the name of your IC Repository database. This name must be the exact name that you gave your IC Repository database. For example, type **`repository`**.

5. Select **File** > **Save** to save the ADL file. Do not close the file.

Creating the CCQ database

These steps create the schema for the CCQ database and seed the database with the configuration data in the `seed.cfg` file. You do not need to modify the seed file.

The seed data contains system data for the Web Management servers and Web Self-Service. You must seed the CCQ database with this data if your system includes Web Management and Email Management.

To create the CCQ database

1. Select **File** > **Database Administration**.
2. From the **DB Connection Set** list, select **DefaultDBConnectionSet**.

3. Enter the information for the fields mentioned in the following table:

Field	Database type	Recommended entry
Configure	SQL Server	Select **Configure**.
	Oracle	Select **Configure**.
	DB2	Select one of the following options: • If you have run the `db2crdb.sh` script to create the database, *or* if you have already configured an IC database, select **Schema Only**. • If you have not run the `db2crdb.sh` script *and* if you have not yet configured an IC database, keep **Schema Only** unchecked and select **Configure**.
Import Seed Data	All database types	Check this box.

4. If the fields in the following table do not have entries, re-type your IC Manager account and password:

Field	Recommended entry
Login Id	Type your IC Manager login ID. **Note:** Do not use your DBA login ID and password.
Password	Type your password.

5. Click **Run** to configure the database.

   Database Designer pauses briefly between configuring the database and importing the seed data.

6. Click **Close**. Do not close the ADL file.

Generating the Interaction Center application

You generate the Interaction Center application to initialize the database with the ADL and version information and to create the Interaction Center data source.

If you are configuring a localized version of IC, you must import the localized seed data after you perform this step. For more information, see Importing localized seed data on page 509.

To generate the Interaction Center application:

1. In Database Designer, select **File** > **Generate Windows Application**.

   The **Generate Windows Application** dialog box opens.

2. Enter the information for the fields mentioned in the following table:

Field	Recommended entry
Messages	Select this check box.
Avaya IC Scripts	Select this check box.

3. If the IC system includes Avaya Agent, enter the information for the fields mentioned in the following table:

Field	Recommended entry
Avaya Agent Layout	• Select this check box. • Type the path and file name for the layout file, as follows: *IC_INSTALL_DIR*\IC73\design\QConsole\avaya_agent_<*lang*>.cdl where <*lang*> is the language of the agent desktop. For example, if Avaya Agent is in English, select avaya_agent_en.cdl
EDU Layout	• Select this check box. • Type the path and file name for the layout file, as follows: *IC_INSTALL_DIR*\IC73\design\QConsole\eduviewer_<*lang*>.xsl where <*lang*> is the language on the agent desktop. For example, if Avaya Agent is in English, select eduviewer_en_US.xsl

   For more information about Avaya Agent layouts in non-English languages, see Configuring Avaya Agent for a supported language on page 507.

4. From the **Name** list, select **interaction_center**.
5. Type the path for the directory where you want Database Designer to store the application files.

   For example, type AVAYA_IC73_HOME\apps.

   If you do not know the path, click the **Ellipsis** (**…**) button and navigate to the directory.

6. From the **DB Connection Set** drop-down list, select **defaultDBConnectionSet**.

7. If the fields in the following table do not have entries, re-enter your IC Manager account and password:

Field	Recommended entry
Login Id	Type your IC Manager login ID. **Note:** Do not use your DBA login ID and password.
Password	Type your password.

8. Click **OK**.

   Database Designer creates a new folder with the same name as the application in the target directory. This folder contains the Interaction Center ADL files.

9. Select **File** > **Exit** to close Database Designer.

Chapter 7: Installing IC licenses

Avaya Interaction Center (IC) components do not run if you do not install the license server, and obtain the appropriate license file. For information on how to obtain a license, see *Avaya IC Installation Planning and Prerequisites*.

If IC components cannot access the License server and WebLM, agents may not be able to log in, and servers may not be able to start.

To provide redundant operation in the event of network or WebLM failure, a grace period of 30 days is provided to rectify the failure. The WebLM failure can be when the WebLM system is down, or the WebLM service is down, or the License file in the WebLM service is corrupted or expired.

Note:

For the License Server to enter in a grace period, the License Server must communicate with WebLM at least once.

To configure IC licensing, perform the steps in the following topics:

1. Before you configure IC licenses on page 154
2. Configuring the Web License Manager on page 155
3. Installing the license file on page 165
4. Configuring the License server on page 167
5. Changing the administrative password on page 168

This section also includes the following topics:

- Managing users on page 169
- Viewing server properties on page 170
- Viewing information about configured licenses on page 170

Before you configure IC licenses

Before you install and configure WebLM:

1. You require an application to unzip the war file on the system where WebLM will be deployed.
2. Obtain a license file for your IC components from Avaya, as described in *Avaya IC Installation Planning and Prerequisites*.

3. Install and configure all prerequisite software and hardware, including a Web server and a JDK, as described in *Avaya IC Installation Planning and Prerequisites*.
4. On Solaris system, install a Windowing environment such as X-Windows on the system that hosts the WebLM.
5. On AIX system, install a Windowing environment such as X-Windows on the system that hosts the WebLM.
6. Install and configure an IC server environment on a system that hosts the WebLM.

Note:

For supported version of WebLM see *Avaya Interaction Center and Avaya Operational Analyst Overview and Specification Guide*.

Configuring the Web License Manager

The Web License Manager (WebLM) is a Web application that hosts your IC license. You must configure the WebLM on each system that hosts an IC or OA license. You must use the **Web** tab of the Configuration Tool to configure the WebLM. This section is only applicable when you deploy the WebLM war file shipped with IC.

This section describes how to install and configure the Web License Manager for each operating system that IC supports. This section includes the following topics:

- Hosting multiple Web applications on one system on page 155
- Advanced properties for the Web LM on page 156
- Viewing license pick usage on page 156
- Configuring the WebLM on Windows on page 156
- Configuring the WebLM on Solaris on page 159
- Configuring the WebLM on AIX on page 162

Hosting multiple Web applications on one system

If the IC system includes more than one Web application on the same system as the WebLM, You should configure all of the Web applications on the target system at the same time.

Important:
If you do not configure all of the Web applications simultaneously, keep all the Web applications options on the target system selected when you re-run the Configuration Tool to create the new Web applications. If you do not keep the options for previously created Web applications selected, the Configuration Tool might delete those Web applications.

Advanced properties for the Web LM

The **Web** tab also includes the advanced properties for the Java Virtual Machine.

Configure the advanced properties only if you expect a high volume of traffic for the Web License Manager. For more information, see Configuration Tool advanced properties on page 520.

Viewing license pick usage

In the Web License Manager, by clicking the product link in the left pane, you can view the licenses you have acquired for each feature in the product. You can also view the pick usage of the license for each feature in a product. For example, if the total number of licenses for a given feature is 10 and if 5 licenses are only used, then pick usage is displayed as 5/50%.

Configuring the WebLM on Windows

Use these instructions to host the WebLM on a Windows system. You do not need to stop the IIS Web server on Windows systems.

1. Run the Configuration tool on page 156.
2. Extracting the WebLM war file before starting the Avaya IC WebLM Service on page 158.
3. Starting the Avaya IC WebLM service on page 158.

Run the Configuration tool

To configure the Web License Manager to run on a Windows system:

1. Start the Configuration Tool by selecting **Start** > **Programs** > **Avaya Interaction Center** 7.3 > **Configuration Tool**.
2. Log in with your IC Manager login ID and password.

3. On the **Web** tab enter the information for the fields mentioned in the following table:

Field	Description	Sample entry
Tomcat Base Port	The port used to configure the following ports: Tomcat HTTP ports for Web applications. Tomcat AJP (Web server connector) ports.	Default: 9600
IIS Website	The name of the IIS Web server that the Web application will use. **Note:** For a localized version of IIS, type the localized name for the IIS Web server.	Default Web Site
Web Server Host	The name of the system that hosts the Web server. Do not include the DNS domain.	testbox
DNS Domain	The network (DNS) domain of the system that hosts your Web server. Do not enter an IC domain. **Note:** Verify the default DNS domain carefully to ensure that it is correct.	xyzcorp.com
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: HTTP port is 80. HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application on each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: **`http://<server>.<domain>.com:9600/ictest`** Note: The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Select the box

4. Select the **Configure Web License Manager** check box.

5. Enter the information for the fields mentioned in the following table:

Field	Description	Sample entry
SSL Port for WebLM	The port used to configure the Web License Manager server	Default: 8443 In IC 7.3.2 and later, the default port is 52233.
Log File Location for WebLM	Enter the directory where weblmserver.log file must be saved. Ensure that the path you specify exists.	Default: AVAYA_IC73_HOME \tomcat\webapps\ WebLM\data\log
Log File Maximum Backup Index	The maximum number of the weblmserver log files that can be created.	Default: 1
Log File Maximum File Size (in MB)	The maximum size of a weblmserver log file.	Default: 10-MB
License Allocation Backup File Size (in MB)	The maximum file size of the License allocation backup file. This file is not used.	Default: 10-MB
Web License Manager JVM Options	This parameter is available only when you right-click in the Config tool and select Show Advanced Properties option.	-Xms256m -Xmx512m -Xss512k

6. Click **Apply Settings**.
7. Click **OK**.
8. Click **Exit**.

Extracting the WebLM war file before starting the Avaya IC WebLM Service

Before starting the IC WebLM service, you must extract the WebLM war file:

1. Create an empty WebLM folder inside the webapps folder located at AVAYA_IC_HOME\ tomcat\webapps IC Core Server.
2. Open WebLM.war using an unzip tool and extract the contents of WebLM.war to newly created WebLM folder.

Starting the Avaya IC WebLM service

You must extract the WebLM war file before starting the WebLM service.

Note:

If you do not perform the steps provided in Extracting the WebLM war file before starting the Avaya IC WebLM Service section, the WebLM server will not start when started for the first time and will give the following error: `SEVERE: Failed to load keystore type PKCS12 with path /Avaya/IC73/tomcat/webapps/WebLM/WEB-INF/weblmserver.p12 due to /Avaya/IC73/tomcat/webapps/WebLM/WEB-INF/weblmserver.p12 (No such file or directory).`

To resolve the error you will need to restart the WebLM service

1. Open the Windows Services control panel.
2. Start **Avaya IC WebLM Service** 7.3.

   For more information about how to start and stop Web application services, see Starting and stopping IC services on page 114.

Configuring the WebLM on Solaris

Use these instructions if you plan to host the WebLM on a Solaris system.

Important:
To configure the Web License Manager on Solaris, you must log in as a user with write permissions on the Web server directories and the IC installation directories. The root user has these write permissions.

To configure the Web License Manager to run on a Solaris system:

1. Start the Configuration Tool:
   a. Navigate to *IC_INSTALL_DIR*/IC73/bin
   b. Run **./configure**
2. Log in with your IC Manager login ID and password.

3. On the **Web** tab enter the information for the general fields mentioned in the following table:

Field	Description	Sample entry
Tomcat Base Port	The port used to configure the following ports: • Tomcat HTTP ports for Web applications. • Tomcat AJP (Web server connector) ports.	Default: 9600
Web Server Home	This field is not applicable if you are only configuring WebLM service with this server. You can specify any path for the Web Server Home if you want to only configure WebLM component of AIC on this server. If you are configuring Website and WebLM on the same server then you must provide the path of the iPlanet Web server.	
Web Server Name	If you are only configuring WebLM service on the same server, then specify the FQDN of server host. If you are configuring Website and WebLM on the same server then you must provide the root name of the server as found in the Oracle iPlanet Server home directory. **Note:** Do not include **`https-`** in the Web server name.	testbox.xyzcorp.com
Web Server Host	The name of the system that hosts the Web server. Do not include the DNS domain.	testbox

Field	Description	Sample entry
DNS Domain	The network (DNS) domain of the system that hosts your Web server. Do not enter an IC domain. **Note:** Verify the default DNS domain carefully to ensure that it is correct.	xyzcorp.com
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: • HTTP port is 80. • HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80

4. Select the **Configure Web License Manager** check box.
5. Enter the information for the fields mentioned in the following table:

Field	Description	Sample entry
SSL Port for WebLM	The port used to configure the Web License Manager server.	Default: 52233
Log File Location for WebLM	Enter the directory where weblmserver.log file needs to be saved. Ensure that the path you specify exists.	Default: *IC_INSTALL_DIR* /IC73/tomcat/webapps/WebLM/data/log
Log File Maximum Backup Index	The maximum number of the weblmserver log files that can be created.	Default: 1
Log File Maximum File Size (in MB)	The maximum size of a weblmserver log file.	Default: 10-MB
License Allocation Backup File Size (in MB)	The maximum file size of the License allocation backup file. This file is not used.	Default: 10-MB
Web License Manager JVM Options	This parameter is available only when you right-click in the Config tool and select Show Advanced Properties option.	-Xms256m -Xmx512m -Xss512k

6. Click **Apply Settings**.
7. Click **OK**.
8. Click **Exit**.
9. To complete the configuration, perform the following steps to ensure that all WebLM services start properly:
   a. In the Oracle iPlanet Server installation directory:
      - Open the admin-server directory.
      - If the directory includes a file called start-ICEnv.backup, execute the following command to rename the file:

        mv start-ICEnv.backup oldstart-ICEnv

   b. Start the Oracle iPlanet server that hosts the Web License Manager application with the following start script:

      <iplanet_home_dir>/https-instance_name/bin/startserv

   c. Navigate to the *IC_INSTALL_DIR*/IC73/bin directory.
   d. Use the following script to start Tomcat:

      nohup ./ictomcat.sh start weblm

Important:
For Solaris only, the Configuration Tool changes the ownership of the implementation file (vesp.imp) and the interface file (vespidl.pk) to root. If you do not want to run IC as root, you must change the ownership of these files as described in Changing the ownership for IC on page 49.

Configuring the WebLM on AIX

Use these instructions if you plan to host the WebLM on an AIX system.

Important:
To configure the Web License Manager on AIX, you must log in as a user with write permissions on the Web server directories and the IC installation directories. The root user has the write permissions.

To configure the Web License Manager to run on an AIX system:

1. Start the Configuration Tool:
   a. Navigate to *IC_INSTALL_DIR*/IC73/bin
   b. Run **./configure**
2. Log in with your IC Manager login ID and password.

3. On the **Web** tab enter the information for the general fields mentioned in the following table:

Field	Description	Sample entry
Tomcat Base Port	The port used to configure the following ports: • Tomcat HTTP ports for Web applications. • Tomcat AJP (Web server connector) ports.	Default: 9600
Web Server Home	The installation path for the IBM HTTP server instance that hosts the Web application.	`/usr/HTTPServer`
Web Server Name	A Solaris-only field. Not applicable for AIX.	Leave this field blank.
Web Server Host	The name of the system that hosts the Web server. Do not include the DNS domain.	testbox
DNS Domain	The network (DNS) domain of the system that hosts your Web server. Do not enter an IC domain. **Note:** Verify the default DNS domain carefully to ensure that it is correct.	xyzcorp.com
Web Server Port	The port that your Web server uses for communication. Ensure that the port matches the protocol used by your Web server for communication. The default ports are: • HTTP port is 80. • HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80

Field	Description	Sample entry
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application on each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: **`http://<server>.<domain>.com:9600/ictest`** **Note:** The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Select this box

4. Select the **Configure Web License Manager** check box.
5. Enter the information for the fields mentioned in the following table:

Field	Description	Sample entry
SSL Port for WebLM	The port used to configure the Web License Manager server.	Default: 8443
Local File Location	Enter the directory where weblmserver.log file needs to be saved. Ensure that the path you specify exists.	Default: *IC_INSTALL_DIR*/IC73/tomcat/webapps/WebLM/data/log
Log File Maximum Backup Index	The maximum number of the weblmserver log files that can be created.	Default: 1
Log File Maximum File Size (in MB)	The maximum size of a weblmserver log file.	Default: 10 MB
License Allocation Backup File Size (in MB)	The maximum file size of the License allocation backup file. This file is not used.	Default: 10 MB

6. Click **Apply Settings**.
7. Click **OK**.
8. Click **Exit**.

9. To complete the configuration, perform the following steps to ensure that all WebLM services start properly:
   a. Navigate to the *IC_INSTALL_DIR*/IC73/bin directory.
   b. Use the following script to start Tomcat:

      nohup ./ictomcat.sh start weblm

Important:
For AIX only, the Configuration Tool changes the ownership of the implementation file (vesp.imp) and the interface file (vespidl.pk) to root. If you do not want to run IC as root, you must change the ownership of these files as described in Changing the ownership for IC on page 49.

Installing the license file

After you obtain the license file, install the file in the WebLM. For more information on how to obtain a license file, see *Avaya IC Installation Planning and Prerequisites*.

CAUTION:
Do not change your license file after you receive it from Avaya. WebLM does not accept modified licenses.

To install the license file:

1. In your Web browser, navigate to the following URL for the WebLM:
   `https://<system_name>.<domain>:<webLM_port>/WebLM/LicenseServer`

   For example, : `https://testbox.xyzcorp.com:52233/WebLM/LicenseServer`

   Note:
   The URL for the WebLM is case-sensitive.

   If your contact center uses a proxy server or enhanced security for Internet Explorer, include the proxy server address in the browser exception list and the trusted sites list.

   Note:
   Accessing the URL gives a security alert or error message if you have not generated a security certificate for the WebLM deployment. You can continue to proceed with the Web site by ignoring the error.

2. Click **License Administration**.

   The **Logon** page displays.

3. Enter the default user name and password.

   The default user name is: **admin** and the password is: **weblmadmin**.

   WebLM forces you to change the password immediately to help prevent unauthorized access to your license file. For more information, see Changing the administrative password on page 168.

4. Enter the license file path in the **Enter License Path** field.

   If you do not know the license file path, click **Browse** and select the license file.

5. Click **Install**.

   If the installation is successful, WebLM displays a confirmation page. If you install an incorrect license file, or WebLM cannot access the location of the license file on your network, WebLM displays an error page.

6. In the left pane, click the **aic** hyperlink for Avaya Interaction Center under **Licensed Products**, and confirm that the number of agents and servers matches your expectations.

To install license file on Solaris:

Note:

If you are running WebLM as a non-root user, you must give additional privileges to this non-root user to install the license file.

1. Log in to the Solaris system as root.
2. Execute the following command:

   usermod -K defaultpriv=basic,net_rawaccess <non-root user>.

3. Log in again to the Solaris system as non-root.
4. Start WebLM and install the license file.

To install license file on AIX:

Note:

If you are running WebLM as a non-root user, you must give additional privileges to this non-root user to install the license file.

1. Log in to the AIX system as root.
2. Execute the following command:

   usermod -K defaultpriv=basic,net_rawaccess <non-root user>.

3. Log in again to the AIX system as non-root.
4. Start WebLM and install the license file.

Configuring the License server

This section includes information about how to configure the License server that is automatically installed with the primary ORB server. Use the same configuration parameters in all other License servers in the IC system.

Do not host more than one License server on a system. If your IC system requires multiple License servers, you must host them on different systems.

To configure the License server:

1. In IC Manager, double-click the License server from the list of servers.
2. On the **General** tab enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	License_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the IC domain for the server from the drop-down list.	For example, select **Default** from the drop-down list if the server is in the Default domain.
Host	Select the IP address of the system from the drop-down list, or type the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

3. Click the **License Server** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Warn about upcoming license expiry	Select this field.	
Time in advance of expiry (hours)	If you selected Warn about Upcoming License Expiry, enter the amount of time before the license expires that you want to be warned.	Default is 96 hours.

Field	Recommended entry	Notes
Alarm on no licenses	Select this field.	
WebLM Server URLs	Add the URL of the server page for a WebLM License Manager. **Note:** The URL for the WebLM is case-sensitive and the maximum length supported is ten characters.	The default URL is `https://<system_name>.<domain>:<webLM_port>/WebLM/LicenseServer` For example: `https://testbox.xyzcorp.com:52233/WebLM/LicenseServer` **Important:** You must not use the IP address of the system in the URL.

4. Click **OK**.
5. Start the License Server.

   Note:
   Start the License Server after configuring the database applications. For more information, see Configuring databases on page 122.

6. Confirm that the Alarm Monitor at the bottom of the IC Manager window displays a confirmation message, such as `WebLM server in the configuration is working`. If you do not see this alarm message, your license is not working correctly.

Changing the administrative password

The Web License Manager does not impose constraints on the administrative password. However, you can use a combination of alphabetic and numerical characters.

To change the administrative password for Web License Manager:

1. In your internet browser, navigate to the URL of the server page for the WebLM.

   A sample URL is **`https://<system_name>.<domain>:<webLM_port>/WebLM/LicenseServer`**

   The URL for the WebLM is case-sensitive.

2. Click the **License Administration** page.

   The system displays the Logon page.

3. Enter the default user name and password.

   The default user name is: `admin` and the password is: `weblmadmin`.

4. Complete the following fields under **Change Password**:
   - Current password
   - New password
   - Confirm password
5. Click **Submit**.

   The system displays the Logon page. You need to login again with a new password.

Managing users

In Web License Manager (WebLM), you can add new users, configure the existing users, and also delete users. You can view the list of user by clicking the **Manage Users** link in the left pane.

To add a user:

1. In the left pane of Web License Manager page, click **Manage Users**.
2. Click **Add User**.
3. In the right pane, enter the user name in the **User Name** field.

   The user name must be unique.
4. Enter the password and in the **Password** and **Confirm Password** fields.
5. Click **Add User**.

To delete a user:

1. In the left pane of Web License Manager page, click **Manage Users**.
2. Click **Delete User**.
3. In the right pane, select the check box corresponding to the user you want to delete.
4. Click **Delete**.
5. Click **OK** to confirm deleting the selected user.

To modify a user:

Note:
You can modify only the password for a user.

1. In the left pane of Web License Manager page, click **Manage Users**.
2. Click **Modify User**.
3. In the right pane, select the user name from the **User Name** drop-down list.

4. Enter the new password for the selected user in the **Password** and **Confirm Password** fields.

   Note:
   You must enter a valid password to proceed further.

5. Click **Change**.

Viewing server properties

On the WebLM page, you can view the WebLM server properties that include the information about the primary host ID of the WebLM server and also the available host IDs on that server.

You can view the server properties by clicking the **Server Properties** link in the left pane of the WebLM page.

Viewing information about configured licenses

The WebLM page displays the detail license information for a product. You can click the product name link under the **Licensed Products** category to view the information.

The license information displays details about date and time the license file is installed, the licensed features, and acquired licenses. You can also click the **View Peak Usage** link on the page to view the peak usage of the licenses for the features of a product.

When you click the **View Peak Usage** link, the system displays the **View Peak Usage** Web page. This page displays a table that displays the feature-wise peak usage information. The table displays the information in the following columns:

- **Feature (License Keyword):** This column lists the display name of the licensed features of the product and the keywords of each feature. These keywords are used to represent the licensed feature in the license file.
- **Currently Allocated:** This column lists the number of feature licenses purchased by the customer.
- **Usage: qty/%:** This column lists the number of feature licenses for each licensed feature that is currently used by the licensed applications. The column also displays the percentage of usage. For example, if there are 50 available feature licenses and 5 feature licenses have been used by the applications, this column will display 5/10%.
- **Peak Usage (last 7 days): qty/%:** This column lists the highest number of feature licenses for each licensed feature that has been used by the applications in the past seven days. The column also displays the percentage of peak usage. For example, if the peak usage in the past seven days is 25 and the feature licenses those were available during the peak usage calculation was 50, the column displays 25/50%.

- **Peak Usage (last 30 days): qty/%:** This column lists the highest number of feature licenses for each licensed feature that has been used by the applications in the past 30 days. The column also displays the percentage of peak usage. For example, if the peak usage in the past 30 days is 50 and the feature licenses those were available during the peak usage calculation were 50, the column displays 50/100%.
- **Time of Query:** This column lists the date and time when the last usage query for the WebLM server was executed. If the status of the last usage query was Failed, this column also displays the date and time of the usage query that was last successful.
- **Status:** This column lists the success or failure of the last usage query executed for the WebLM server.

Note:

The **Status** column of the WebLM server remains empty if the server has not been queried even once for feature license usage.

Chapter 8: Configuring Telephony

The Avaya Computer Telephony for IC (Telephony) is part of the voice channel of Avaya Interaction Center (IC).

You can use the information provided in this chapter to set up a simple Telephony environment with one Telephony server and one PBX or ACD. IC also supports a complex Telephony environment that can include multiple Telephony servers with multiple PBXs or ACDs and works independently or together as an integrated environment. You can also configure an IVR.

To configure Telephony, perform the steps in the following topics:

1. Before you configure Telephony on page 173
2. Configuring the ACD name parameter on page 173
3. Creating the Telephony server on page 174
4. Creating a voice queue on page 178
5. Creating the Telephony Queue Statistics server on page 183
6. Starting the Telephony servers on page 185
7. Configuring a Workflow server for Telephony on page 186
8. Building and loading workflow for Telephony on page 189
9. Creating routing hints for the Incoming Call workflow on page 191

Your IC system can also include the following optional configurations:

- Multi-site heterogeneous switches, as described in *Avaya IC Telephony Connectors Programmer Guide*.
- Return on No Answer (RONA), as described in *Avaya IC Telephony Connectors Programmer Guide*.
- Connections to an IVR and VP, as described in the *IC Integration with VP/IR Guide*.
- Connection to Siebel, as described in the *Siebel Integration Guide*.

Before you configure Telephony

Before you configure Telephony and related components, make sure that you:

1. Install and configure all prerequisite software and hardware. The prerequisites can include one or more of the following:
   - Database
   - Telephony switch, equipment, and software
   - IVR (optional)

   For more information about the prerequisites and supported platforms for Telephony, see *Avaya IC Installation Planning and Prerequisites*.
2. Copy the IC server files to the target systems, as described in Installing IC server components on page 35.
3. Configure a secondary server environment, as described in Configuring the ORB server environment on page 44.
4. Perform all the steps to configure the IC core servers, databases, and related components, as described in Configuring core servers on page 83.

Configuring the ACD name parameter

You must configure an ACD name parameter for each ACD in your IC system. You can include identifying information, such as department or site in the ACD name.

To configure the ACD name parameter:

1. In IC Manager, click the **Configuration** tab.
2. In the left pane, select **Telephony** > **ACD Name** from the list of tables.
3. On the toolbar, click **New**.
4. In the **ACD Name** field, type the name for the ACD.

   Use alphanumeric characters without spaces and special characters.
5. Click **Ok**.
6. Refresh the Directory server:
   a. Select **Manager** > **Refresh**.
   b. Click **Ok**.

   If you do not receive a Success message, perform the steps in Troubleshooting the refresh in IC Manager on page 499.

Creating the Telephony server

The Telephony server (TS) is the connector server for the voice channel. The Telephony server interfaces with a switch (PBX), monitors phone calls, and controls telephony routing. This server uses the EDU server to record information on telephone calls. The Telephony server is specific to the switch you are using.

This section describes how to set up a Telephony server for a single site that does not receive more than 10,000 voice contacts per hour. For more information about the Telephony server, see *Avaya IC Telephony Connectors Programmer Guide*.

For information about how to configure the VDN, CDN, or CCT on each link of the switch to communicate with the Telephony server, see *Avaya IC Installation Planning and Prerequisites*.

To create a Telephony server:

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **TS**.
3. Click **Ok**.
4. On the **General** tab enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	TS_<*domain*>_<*switch*>	Include the name of the domain and the name of the switch in the server name to identify the server.
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Voice1` from the drop-down list if the server is in the Voice domain.
Host	Select the IP address of the system from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. Click **Ok**.

6. Configure the telephony switches mentioned in the following table to complete the Telephony server configuration.

Telephony switch	Location of step
Avaya Communication Manager	Configuring the Telephony server for Avaya Communication Manager on page 175
SIP	Configuring Telephony Server for SIP on page 176

Configuring the Telephony server for Avaya Communication Manager

For information about the interface between Avaya products and the IC Telephony server, see *Avaya IC Telephony Connectors Programmer Guide*.

Tip:
This section includes only the basic required properties. You can also configure advanced properties or properties on the **Configuration** tab. For example, you can add a parameter to handle blocked ANIs. For more information, see *Interaction Center Administration Guide* and *Avaya IC Telephony Connectors Programmer Guide*.

To configure the Telephony Server for Avaya Communication Manager:

1. In IC Manager, double-click the Telephony Server (TS) from the list of servers.
2. Click the **TS** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
ACD Name	Select the name of the ACD assigned to the Avaya switch.	The name of the ACD that this TS is serving from a pick list of names assigned to the ACD during system configuration.
ACD Type	Select Avaya	The type of ACD with which the TS communicates.
ACD Model	Select Definity	The model of the ACD that corresponds to the selected ACD Type.

Field	Recommended entry	Notes
ACD Protocol	Select asai	The protocol to be used between the TS and the ACD. If your system includes a Legacy TS with switch with Avaya DEFINITY software, see *IC/OA Software Upgrade and Data Migration*.
Site	Select the site of your TS.	Select the site that this server is associated with. The TS uses this information to retrieve the queues for internal monitoring.
ACD Link	Enter the IP address or the host name (if the host name can be resolved) of AES.	The device through which the TS communicates with the ACD. Maximum length is 32.
Signal Number	Specify a signal number when configuring multiple Avaya users on a single system. There is no default value in the TS, but IC Manager sets this value to 1. Maximum length is 16.	The signal extension number of the ASAI line associated with each TS. The signal number is mandatory. If the signal number is not specified, the TS cannot establish the link between users.
Call Control	Select to enable call control on every call.	If selected, enables the TS to monitor calls, not stations, on the system.

3. Click **Ok**.

Configuring Telephony Server for SIP

This section describes the required and optional parameters that must be set to configure the SipTS in IC Manager.

To configure the SipTS in IC Manager:

1. In IC Manager, click the **Server** tab.
2. On the toolbar, click **Create Server**.
3. From the list of servers, select the **TS** server type.
4. Configure the following parameters at the appropriate tabs and click **Ok**.

General tab

The settings on the **General** tab pertain to the Communication Manager switches supported in IC 7.3:.

Field	Recommended entry	Notes
Name	TS_SIP	The name assigned to the TS.
Domain	Select the SIP (IC) domain from the drop-down list.	The server is assigned to the SIP (IC) voice domain.
Host	Select the IP address of the system from the drop-down list. Enter the IP address if it is not in the list.	After selecting the Host, IC Manager fills in the fields for Directory, Port, and Executable.
Executable	Path and file name of the sipsrv.exe file.	Verify this field is pointing to the new SipTS executable.

TS tab

The settings on the TS tab pertain to Communication Manager switches supported in IC 7.3:

Field	Recommended entry	Notes
ACD Name	Select the name of the ACD assigned to the switch.	The name of the ACD (switch) that this TS is serving from a pick list of names assigned to the ACD during system configuration.
ACD Type	Select SIP	The type of ACD with which the TS will communicate.
SBC Type	Select CM	The model of the ACD that corresponds to the selected ACD Type.
ACD Protocol	Select SIP	The protocol used by the Application Link Server to communicate with the TS and the switch.
Site	Select the site of your TS.	The site that this TS is associated with. The TS uses this information to retrieve the queues for internal monitoring.
SIP B2B Device	User name of single B2BUA within the SipTS. For example, 62011.	This is mandatory property. **Note:** One SIP TS can have only one B2BUA.
SIP B2B Password		Password for the `B2BUA`.

Comments on this document? infodev@avaya.com

Field	Recommended entry	Notes
SIP Domain	The IP address or FQDN of the SIP Registrar.	This is mandatory property.
SIP Fail Device	The route point or phone number, for example, 47000.	This is mandatory property. It cannot be the park device with wait treatment style 1.
SIP Out-bound Proxy	The IP address or FQDN of the SIP Proxy.	This is mandatory property. The address must be a valid SIP URI and starts with `sip`, for example `sip:135.8.52.125`.
SIP Protec-tion Domain	The SIP domain name	This is an advanced and mandatory property. The required format is: `sip:avaya.com` The property is used for Digest Authen-tication.
SIP Route-Point Pass-word		The common password for all route points configured in any TSA.

Advocate tab

The settings on this tab pertain to the Communication switches supported in IC 7.3:

Field	Recommended entry	Notes
Enable Advocate	Select to enable Business Advocate. by default it is cleared.	Selecting this parameter displays the other parameters listed in this table.
Default RONA Destination	No Selection	
Optional Backup Link for Advocate	No Selection	

Creating a voice queue

The sample Incoming Call workflow uses the DefaultVoiceQueue@DefaultTenant voice queue. Create this queue and additional queues, including a queue for each possible route (transfer) point where the Incoming Call workflow can route a voice contact.

IC uses voice queues for the following:

To gather statistics information: The TSQueueStatistics server monitors the queues and maintains statistics in the ADU server. These statistics can then be processed by, for example, OA. For more information, see Creating the Telephony Queue Statistics server on page 183.

To provide a literal translation for a switch device: With this literal translation, you can reference a destination in the switch. For example, you can reference VDN 1234 as queue_sales. IC displays queue_sales as a destination in the Unified Agent Directory.

To provide support for multi-site heterogeneous switches: IC uses the information you enter in the fields on the Voice tab of the queue to support multi-site heterogeneous switches. For more information, see *Avaya IC Telephony Connectors Programmer Guide*.

To integrate with routing hints: You add the ID of the voice queue to the RoutingHint table when you configure the routing hints used by the Incoming Call workflow. For more information, see Creating routing hints for the Incoming Call workflow on page 191.

The following procedure explains how to create a simple voice queue. For more information, including queues for transfers and multi-site heterogeneous switches, see *Interaction Center Administration Guide* and *Avaya IC Telephony Connectors Programmer Guide*.

To create a simple voice queue:

1. In IC Manager, click the **Device** tab.
2. Select **Device** > **New Device**.
3. In the **New Device** dialog box, select **Voice Queue**. Click **OK**.
4. In the **Device Editor (Voice)** dialog box:
   a. Click the **General** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Description
ID	The device number known to the PBX or ACD.	The ID is the VDN or vector identifier that your PBX or ACD uses for the queue. The ID must be a numeric value.
Site	Select the site of your Telephony server.	
ACD Name	Select the name of the ACD.	This is the ACD Name that you confirmed in Configuring the ACD name parameter on page 173,

Field	Recommended entry	Description
Name	Type a name for the voice queue.	For the default voice queue, type DefaultVoiceQueue @DefaultTenant. Queue names can have up to 256 characters, including special characters and spaces. Queue names cannot: • Start with a digit, such as zero (0). • Start with an asterisk "*" or a pound sign "#". • Contain "@" except default queue. The Unified Agent Directory displays this name to agents.
Media	Voice	Automatically set by IC Manager. You cannot change this field.
Priority	Assign a priority to the queue.	For example, type 1.
Service Level	Type the number of hours, minutes, and seconds in the format HH:MM:SS	The service level defines the time within which all voice contacts in the queue must be answered. Type the time in the HH:MM:SS format.
Minimum agents	1	Type the minimum number of agents who must be active to use the queue.
Addressable	Select this box.	Determines whether the queue is displayed in the Unified Agent Directory.

b. Click the **Voice** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Description
Enable EDU Tracking	By default it is cleared.	If selected, the first Telephony server in the TS Set monitors this queue internally. Select this option only under one of the following conditions: • The switch and CTI link cannot make a call-to-data association. • The switch supports queue monitoring. • The environment is configured to ensure that new contacts are pre-processed by one Telephony server, where all the queues reside, but all agents are handled by another Telephony server. Usually the pre-process has to do with call routing and queue monitoring. **Note:** In addition to selecting this check box, make sure that the associated Telephony server is the first one in the TS Set list.
Wait Treatment Style	Leave this field blank.	The numeric value associated with the wait treatment configuration on the switch. For more information, contact your switch administrator. The field 'Wait Treatment Style' is not present in the Voice tab while creating devices.

Field	Recommended entry	Description
TS Set	Select the **Ellipsis (…)** button and in the dialog box: • Select **New**. • Select the Telephony server that handles voice contacts for this queue from the drop-down list. • After you have added all of the Telephony servers, click **Ok**.	Defines the Telephony servers that can be used to deliver voice contacts to this queue, and the order that the Multi-Site Heterogeneous Switch (MSHS) mechanism follows when attempting to deliver contacts to specific queues. In order to do this, the MSHS uses the ADU for its central data store. The TS Set can only include Telephony servers that handle contacts from the switch where the queue resides. The value of TS Set is stored in the `voicets_set` field of the `dbo.queue` table in the `repository` database. If the cumulative size of the Telephony Server names that you add in TS Set exceeds the default size of the `voicets_set` field, ICManager might display an error message ***Error while applying changes. Internal error***. The default size of the `voicets_set` field in different databases is as mentioned below: • **MS SQL**: 255 • **IBM DB2**: 765 • **Oracle**: 765 To successfully store the TS Set value in a database, you can either use short names for the Telephony servers that you want to add in TS Set or increase the `voicets_set` field size in the database.

Comments on this document? infodev@avaya.com

Field	Recommended entry	Description
		You must increase the field size only by using the Database Designer application. You must not change the field size directly in the database. For more information about using Database Designer, see *IC Database Designer Application Reference*. **Note:** Queue names are kept in cache for 24 hours.

5. Click **Ok**.

Creating the Telephony Queue Statistics server

The Telephony Queue Statistics server (TSQS) monitors the voice channel and maintains queue statistics in the ADU Server. These statistics include contact count and age of the oldest contact.

Note:
If Business Advocate handles all routing for voice contacts, you do not need a TSQS server.

The IC installation program does not automatically add this server.

To create the TSQS:

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **TsQueueStatistics** and click **OK**.
3. On the **General** tab enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	TsQueueStatistics_<*domain*>	Include the domain in the server name to identify the server.

Field	Recommended entry	Notes
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Voice1` from the drop-down list if the server is in the Voice domain.
Host	Select the IP address of the system from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Configure the telephony switches mentioned in the following table to complete the TSQS server configuration:

Telephony switch	Location of step
Avaya Communication Manager	Configuring the TSQS server for Avaya Communication Manager on page 184

Configuring the TSQS server for Avaya Communication Manager

Tip:
This section includes only the basic required properties. For information about the advanced properties, see *Interaction Center Administration Guide*.

To configure the TSQS for Avaya Communication Manager:

1. In IC Manager, double-click the TS Queue Statistics (TSQS) server from the list of servers.
2. Click the **TSQS** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
ACD Name	Select an ACD Name.	The name of the ACD (switch) that this TSQS is serving. Provides a pick list of name(s) assigned to the switch during system configuration. Each TSQS on the system must have a unique ACD Name.
Site	Select the site where the TSQS is located.	The site used by your TS configured for the Avaya switch.
ACD Type	Select Avaya.	The ACD Type option used by your TS configured for the Avaya switch.

Field	Recommended entry	Notes
ACD Model	Displays Definity after you select Avaya as ACD Type.	The ACD Model option used by your TS configured for the Avaya switch.
ACD Protocol	Select asai.	The ACD Protocol option used by your TS configured for Avaya switch.

3. Click **Ok**.

Starting the Telephony servers

Important:
Create the voice queues before you start the Telephony server and the TSQS server.

To start Telephony servers:

1. Start the Telephony server:
   a. In IC Manager, select and right-click the Telephony server.
   b. Select **Start**.

   After the Alarm Monitor displays a message confirming that the server has started correctly, continue with the next step.
2. Start the TSQS server:
   a. In IC Manager, select and right-click the **TSQS server**.
   b. Select **Start**.

   After the Alarm Monitor displays a message confirming that the server has started correctly, continue with the next step.
3. Set your Telephony server to start automatically
   a. In IC Manager, double-click the Telephony server from the list of servers.
   b. Click the **General** tab.
   c. Select the **Auto Start** check box.
   d. Click **Ok**.
4. Set your TSQS server to start automatically
   a. In IC Manager, double-click the **TSQS server** from the list of servers.

b. Click the **General** tab.

c. Select the **Auto Start** check box.

d. Click **Ok**.

Configuring a Workflow server for Telephony

To create and configure a Workflow server for Telephony, perform the steps in the following topics:

1. Creating a Workflow server for Telephony on page 186
2. Configuring the voice channel for the Workflow server on page 187

If the IC system includes multiple Workflow servers, perform these steps on each Workflow server that processes voice contacts.

Creating a Workflow server for Telephony

These instructions only provide information about those parameters you need to set when you create a Workflow server to handle voice contacts. For more information about the other parameters in the Workflow server, see Configuring multiple Workflow servers on page 94 and *Interaction Center Administration Guide*.

To create a Workflow server for Telephony:

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **Workflow**.
3. Click **Ok**.
4. Click the **General** tab, and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	Workflow_<*domain*>	Include the domain in the server name to identify the server.

Field	Recommended entry	Notes
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Voice1` to use the pre-configured domain for Telephony.
Host	Select the IP address of the system from the drop-down list, or type the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. Click the **Workflow** tab.
6. From the **IC Data Source** drop-down list, select the Interaction Center data source.

   The default name for the data source is interaction_center. This is the data source that you created in Generating the Interaction Center application on page 151.
7. Select **Synchronous Startup Flows**.
8. If the following row does not exist, add it to the Synchronous Startup Flows:
   a. Select **New**.
   b. In the new row, type **`web_routing.update_qw_cache`**
   c. Click **Ok**.
9. Continue with Configuring the voice channel for the Workflow server on page 187.

Configuring the voice channel for the Workflow server

To configure the voice channel for the Workflow server:

1. In the **Server Editor** for the Workflow server, click the **Channels** tab.
2. On the toolbar, click **New Channel**.

3. In the **Channel Editor** dialog box, enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Global	Do not select this field.	Do not select this field to create a channel for a specific server or media, such as Telephony.
By Server	• Do not select this field if you want this channel to handle events from all servers of the type that you select from the **Service** drop-down list. • Select this field if you want this channel to handle events from only one specific server that you select from the **Service** drop-down list.	If you select this field, and you need this Workflow server to communicate with more than one server, you must create another channel for that server. **Warning:** If you select this field and the Telephony server is named "TS", the Workflow server cannot communicate with the Telephony server.
Channel Range	No entry necessary.	Completed by IC Manager
Service	Select **TS** or a specific Telephony server from the drop-down list.	Whether you can select a server or a type of server, depends on whether or not you selected the **By Server** field.
Criteria	Type the criteria you want the workflow to use for the event.	For example, you can enter a criteria for the workflow to route calls that arrive at a routing point. For a detailed description of the criteria for each server and server type, see the description of the `Assign` method in the Programmer Guide for that server. For example, to see criteria for the Telephony server, see *Avaya IC Telephony Connectors Programmer Guide*.

4. Click **Ok**.
5. Select the channel that you have created.
6. On the toolbar, click **New Association**.

7. In the **Channel Association** dialog box, enter the information for the fields mentioned in the following table:

Field	Recommended entry
Channel Range	Completed by IC Manager
Service Interface	Completed by IC Manager
Event	TS.IncomingCall **Note:** This field is case-sensitive.
Flow	Type `<workflow_project>.<routing_workflow>` For example, if you use the sample Incoming Call workflow, type `ts.incomingcall` **Note:** This field is case-sensitive.

8. Click **OK**.
9. Click **OK**.
10. On the **Server** tab of IC Manager, select the Workflow server that handles voice contacts.
11. Right-click the Workflow server and select **Start**.

Building and loading workflow for Telephony

You can use the sample workflows to configure and test your Telephony servers. When you move into production, modify the properties of the sample workflows to meet your system needs and configuration. For more information about the sample workflows and ways to customize them, see *Avaya IC Media Workflow Reference*.

For each workflow project, perform the steps in the following topics:

1. Building the Incoming Call workflow on page 190
2. Loading workflows in the Workflow server on page 190

Building the Incoming Call workflow

You do not need to configure any blocks to use the sample Incoming Call flow.

To build the Incoming Call workflow

1. In Workflow Designer, select **File** > **Open Project** and open the TS project.

   You can find the TS project in the following directory: *IC_INSTALL_DIR*\IC73\design\IC\Flows\Avaya\TS\TS.prj
2. Double-click `incomingcall.qfd` in the **Project** pane.
3. Select **Project** > **Settings**.
4. Click the **Database** tab and enter the values for the following fields:
   - **IC Data Source**: Interaction Center Data Source name.
   - **Login ID**: Valid IC Administrator account

     The default account is Admin.
   - **Password**: Password for the account
5. Click **Ok**.
6. Select **Build** > **Build Flowset**.

   Workflow Designer verifies and compiles the flows. All error messages, including the block name, script name, and offending line, are displayed in the Output bar.
7. Select **File** > **Exit** to exit Workflow Designer.

Loading workflows in the Workflow server

When you build a flowset, Workflow Designer does not automatically load and run the workflows in the Workflow server. You can reload workflows without restarting the Workflow server.

Tip:
Test the workflows and confirm that they work correctly. If the Workflow server is not running the new workflows, stop and restart the server.

To reload workflows in the Workflow server:

1. In IC Manager, click the **Servers** tab and double-click the Workflow server.
2. In the **Workflow server** settings dialog box, click the **Workflow** tab.
3. Select **Reload Flows**.

4. In the **Reload Flows** dialog box:
   a. Select **Force Immediate Reload**.
   b. Click **Ok** to reload all currently loaded workflows even if the versions are same.
5. Click **Ok**.

Creating routing hints for the Incoming Call workflow

The Add Routing Hints (DNIS) block in the Incoming Call workflow uses the routing hints in the RoutingHint table of the Directory server to route incoming voice contacts. The sample Incoming Call workflow requires at least one routing hint for the main incoming DNIS number. Assign this routing hint to a voice queue that you created in Creating a voice queue on page 178.

You can create routing hints for one or more additional DNIS numbers, if required by your contact center.

Important:
Routing hints must be in lower case. Do not use upper and lower case in your routing hints. If the routing hint is not in lower case, the workflow cannot locate the routing hint, and IC cannot correctly route the contact.

Each row in the routing hint table contains the following:

- A routing hint
- The name of the voice queues where contacts that match the routing hint should be routed

For more information about how workflows use routing hints, see *Avaya IC Media Workflow Reference*.

To create routing hints:

1. In IC Manager, click the **Configuration** tab.
2. In the left pane, select **Tables** > **Workflow** > **RoutingHint**.
3. Click **New**.

4. In the right pane, enter the information for the fields mentioned in the following table:

Parameter	Recommended entry	Description
Routing Hint	Type a routing hint.	For the sample Incoming Call workflow, create a routing hint with the DNIS for the incoming calls. For example, if the DNIS is 21000, type 21000 in this field. The routing hint must be a single word in all lower case or a series of numbers. Do not use special characters.
Voice Queue ID	Type the name of a voice queue.	You must not use the DefaultVoiceQueue@DefaultTenant for routing hints. For information on how to create a voice queue, see Creating a voice queue on page 178.
Category/ Qualifier	Leave this field blank.	Business Advocate uses this field.
Tenant	Leave this field blank.	Telephony does not use tenancy.

5. Click **Ok**.
6. Select **Manager** > **Refresh**.

Chapter 9: Configuring Web Management

Web Management is a Web-based marketing, sales, and service application that personalizes and manages Web transactions for Avaya Interaction Center. Configure Web Management if your IC system includes Web Management or Email Management.

This section includes the following topics that describe Web Management and the steps that you must perform to complete the configuration of Web Management:

1. Web Management support for media channels on page 195
2. Before you configure Web Management on page 195
3. Configuring servers for Web Management on page 196
4. Configuring Web Management services on page 206
5. Integrating Web Management Administration on page 226
6. Configuring a Workflow server for Web Management on page 229
7. Using workflows for Web Management on page 232
8. Configuring routing hints for the Qualify Chat workflow on page 234
9. Configuring the ICM server on page 237
10. Configuring IIS server for ICM support on page 239
11. Configuring the Central Internet Routing service on page 240
12. Configuring the Website on page 241
13. Configuring Avaya Full Text Search Engine on page 248
14. Configuring Web Scheduled Callback on page 257
15. Refreshing IC Manager on page 286

This section includes the following topics about optional Web Management configurations:

- Setting up a separate administration Website (optional) on page 277
- Setting up a separate customer Website (optional) on page 279
- Deploying multiple ICM servers (optional) on page 280
- Security configuration on page 287

For information on how to set up RONA for Web Management, see *Interaction Center Administration Guide*.

Web Management support for media channels

The following table shows the integrated functionality that Web Management provides and the support that the functionality provides for the chat channel and the email channel:

Feature or component	Chat channel	Email channel
Customer management	✓	✓
Self-service to provide suggested responses for agents	-	✓
Chat escalation	✓	
Chat typing status	✓	
Web scheduled calls	✓	
Email escalation		✓
Survey	✓	
WebACD server administration	✓	✓
Web page multi-tenancy and multi-tenancy administration	✓	✓
DataWake and DataWake administration	✓	✓
Chat server and client components	✓	

Before you configure Web Management

Before you configure Web Management, ensure that you:

1. Install and configure all prerequisite software and hardware, including a Web server.

   For information on prerequisites required for each system, see *Avaya IC Installation Planning and Prerequisites*.

2. Copy the IC server files to the target system as described in Installing IC server components on page 35.
3. Configure a secondary server environment as described in Configuring the ORB server environment on page 44.
4. Perform all the steps to configure the IC core servers, databases, and related components, as described in Configuring core servers on page 83.

Configuring servers for Web Management

You must add and configure Web Management servers to use Web Management and Email Management. These instructions include only the properties required to get the servers running. For information about other server properties, see *Interaction Center Administration Guide*.

This section describes the Web Management servers and how to configure them.

Note:
Add and configure the servers in the order in which they are presented in the following topics. IC systems that include the email channel, but not the chat channel, do not require the Attribute server.

1. Creating the WebACD server on page 196
2. Creating the Attribute server on page 200
3. Creating the ComHub server on page 202
4. Creating the Paging server on page 204
5. Starting the Web Management servers on page 206

Creating the WebACD server

The WebACD server is also known as the Web Automatic Call Distributor server. The WebACD server works as a call distributor for chat and email contacts. This server assigns tasks to agents and tracks different states of agent interactions. This server uses the Attribute server, Paging server, IC Email server, and ComHub server to complete support operations such as managing agent states and administering agent and contact interactions.

The IC installation program does not automatically add the WebACD server. Web Management and Email Management require the WebACD server.

In the Avaya IC 7.3 release, you can configure two WebACD servers within the WebACD cluster, called `WACD_Cluster`. However, only one WebACD is supported for each system for each domain.

In case of two WebACD servers deployment, you have to configure the ComHub server and Paging server for both the Web domain configured with WebACD server. For example: If Web and Web2 are two domains where you have configured WebACD1 server and WebACD2 server respectively. Then, you have to configure the ComHub and Paging servers in both Web and Web2 domain.

Tip:
On your development system, or if you encounter issues with the WebACD server, set the WACD Log Trace Levels on the **Debug** tab to 100,000.

To create the WebACD server:

1. In IC Manager, select **Server** > **New**.
2. In the right pane, select **WACD** from the list of servers.
3. Click **Ok**.
4. Click the **General** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	WebACD_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Web` from the drop-down list.
Host	Enter or select the IP address from the drop-down list.	When you select the host, IC Manager fills in corresponding Directory, Port, and Executable.

5. Click the **WACD** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Host Name	Enter the name of the system that hosts the WebACD server.	For example, enter TESTBOX.
Domain	Enter the domain of the system that hosts the WebACD server.	For example, enter xyzcorp.com.
Service Port	4010	If you must change this port, see *Avaya IC Installation and Configuration* for a list of the default port numbers used by the other Avaya IC servers. Port conflicts can cause serious problems within the Avaya IC system.
IC Data Source	Select the Interaction Center Data Source.	If you used the default name, select `interaction_center`.

Field	Recommended entry	Notes
WACD Webserver	Enter the name and domain of the system that hosts the Web Administration pages.	For example, enter TEXTBOX.xyzcorp.com. This value should be the same as the 'ChatLoginServer' value in the 'System Configuration'properties.
Port	Enter the port that the IC Webserver uses for connections with Web applications.	Default port is 80 unless you plan to configure SSL for your website. If you must change this port, see Avaya IC Portmatrix guide for a list of the default port numbers used by the other Avaya IC servers. Port conflicts can cause serious problems within the Avaya IC system.
Protocol	Select the protocol that you use to connect to the Website.	Select **`http`** unless you plan to configure SSL for your website. For more information on SSL, see *Avaya IC Installation and Configuration*.
Comhub Host Name	Enter the fully-qualified domain name of the system that hosts the ComHub server.	For example, enter TESTBOX.xyzcorp.com.
Comhub Port	Enter the service port for the Comhub server.	Default service port is 4001. If you must change this port, see *Avaya IC Installation and Configuration* for a list of the default port numbers used by the other Avaya IC servers. Port conflicts can cause serious problems within the Avaya IC system.
Website Context	Enter the name of the Web application used for Web Management.	The default website context is **`website`**.

Field	Recommended entry	Notes
Agent Timeout (secs)	100	If the WebACD assigns a contact to an agent who has turned on the "Wait for agent confirmation before accepting a contact" option in Avaya Agent, then this value specifies the number of seconds that the WebACD server waits for confirmation from that agent before it reassigns the contact to another available agent. For details about setting this option, see the *Avaya Agent User Guide*.
Max Display Tasks	*No recommended entry*	Enter the number of currently active tasks to display per request in the WebACD administration pages.
Task Wrap Timeout (secs)	*No recommended entry*	The WebACD server automatically wraps and completes a task after an customer or agent has timed out. For example, if the Avaya Agent shuts down and the user is forced to end the consultation, the WebACD server waits until the amount of time specified in the wrap-up timeout parameter has passed, then wraps and completes the task.
Interval Between Cleanup (mins)	*No recommended entry*	Enter the period of time that the WebACD should wait between cleaning up threads from timed out and abandoned chat tasks.
Max Allowed Queue Time (mins)	*No recommended entry*	Enter the maximum time that a chat task can stay in a queue before it is considered to be dead or abandoned.

Field	Recommended entry	Notes
Summary Interval (mins)	*No recommended entry*	Enter the period of time that the WebACD should wait between creating summary records. This interval must be an even divisor of 60 (for example, you can use 4, 5, 6, 10, 12, or 15, but you cannot use 8 or 9.) If you set the interval to 5 minutes, then the WebACD writes summaries at 12:00, 12:05, 12:10, and so on.
Requalify Contacts	*No recommended entry*	Enable this option if you want the WebACD server to re-run the Qualify workflow on unassigned tasks.
Default Email Cluster	*No recommended entry*	This is applicable if you want to configure WebACD server for email management.

6. Click **Ok**.

CAUTION:
Do not start the WebACD server till it is added to the WACD Cluster or else, the system might crash.

Creating the Attribute server

The Attribute server acts as a communications bridge between the ICM server and the WebACD server for chats. The Attribute server provides:

- Tracking of user web page browsing sessions for DataWake.
- Web site property event notifications between the website and the ICM server.

If your IC system includes DataWake, or if performance issues exist on the website, you can host a second Attribute server on the website system in the DMZ. If your IC system includes this deployment, configure the secondary ORB server on the system to start automatically.

Note:
You must restart the Attribute Server if you change any of the configuration parameters of the Attribute Server.

The IC installation program does not automatically add the Attribute server. Web Management requires the Attribute server.

To create the Attribute server:

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **Attribute**.
3. Click **Ok**.
4. Click the **General** tab and enter the information for the fields mentioned in the following table.

Field	Recommended entry	Notes
Name	Attribute_<*domain*>	Include the domain in the server name to identify the server in the list of servers.
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Web` from the drop-down list if the server is in the Web domain.
Host	Select the IP address of the system from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. Click the **Attribute** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry
Port	The default port is 2300. If you must change the default port, see Changing the service port for the Attribute server on page 519. Port conflicts can cause serious problems within the IC system.
Enable DataWake Recording	Select this field if: • The IC system includes DataWake • You want this Attribute server to track the Web pages browsed by a Website customer.
Enable ICM Bridge	Select this field.
IC Login	By default, this field uses the **icmbridge** account that is provided with IC. If you have not already done so, change the default password for this account. **Important:** Do not use the Administrative account for IC Manager or any account for which the password may change.

Field	Recommended entry
IC Password	Type the password for the account in the IC Login field.
ICM Servers	• Click the **Ellipsis (…)** button. • In the ICM Servers dialog box: – Click **New**. – Select **Enabled**. – Type the name and domain of the system that hosts the ICM server. For example, TESTBOX.xyzcorp.com. – Accept the default port number or change to an available port. – Click **Ok**.

6. Click the **Configuration** tab.
7. Click **New** on the toolbar.
8. Enter `wacd_cluster_name` in **Name** and `WACD_Cluster` in **Value**.
9. Click **Ok**.

Creating the ComHub server

The ComHub server provides a communications hub for the Web Management and Email Management servers. This server also assists in passing information from a web-based interface to the WebACD server, and helps the WebACD server to respond to agent requests, such as logon or logoff.

The IC installation program does not automatically add the ComHub server. Web Management and Email Management require this server.

In case of two WebACD servers deployment, you must configure the ComHub server for both the Web domains that have the WebACD server configured. For example, if Web and Web2 are two domains where you have configured WebACD1 server and WebACD2 server respectively, then, you have to configure the ComHub server in both Web and Web2 domain.

To create the ComHub server:

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **ComHub**.
3. Click **Ok**.

4. Click the **General** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	Comhub_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Web` from the drop-down list if the server is in the Web domain.
Host	Select the IP address of the system from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. Click the **ComHub** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Host Name	Enter the fully-qualified domain name of the system that hosts the ComHub server.	For example, `TESTBOX.xyzcorp.com`.
Service Port	Accept the default port of 4001 or enter a new port.	If you must change the default port, see Changing the service port for the ComHub server on page 518. Port conflicts can cause serious problems within the IC system.
IC Data Source	Select the Interaction Center Data Source.	If you used the default name, select `interaction_center`.
Threads	Accept the default or enter a number of threads.	The default entry is 10. The number of threads that can be constructed to handle communication tasks.

6. Click **Ok**.

Creating the Paging server

The Paging server serves as a communications bridge between Avaya Agent and the ComHub server. This server brokers messages to ensure that the messages are sent to the correct agents and to the WebACD server through ComHub server.

Important:
When you create IC accounts for agents who handle chat contacts, ensure that the domain for those agents fails over to the domain that includes the Paging server.

The IC installation program does not automatically add the Paging server. Web Management and Email Management require this server.

In case of two WebACD servers deployment, you must configure the Paging server for both the Web domains that have the WebACD server configured. For example, if Web and Web2 are the two domains where you have configured WebACD1 server and WebACD2 server respectively, then, you have to configure the Paging server in both Web and Web2 domain.

To create the Paging server:

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **Paging**.
3. Click **Ok**.
4. Click the **General** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	Paging_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Web` from the drop-down list if the server is in the Web domain.
Host	Select the IP address of the system from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. Click the **Paging** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Host Name	Enter the name of the system that hosts the Paging server.	For example, enter TESTBOX. **Important:** The Avaya IC agent desktop application uses this host name without the "Domain" name to connect to the Paging server. Configure the agent system to use the host name without the domain name suffix to communicate with the system that hosts the Paging server. Starting IC 7.3.3, the Avaya IC agent desktop application uses the FQDN to connect to the Paging server. The agent system should be configured to use the FQDN to communicate with the system that hosts the Paging server.
Domain	Enter the domain of the system that hosts the Paging server.	For example, enter xyzcorp.com. Starting IC 7.3.3, the Avaya IC agent desktop application uses the FQDN to connect to the Paging server. The agent system should be configured to use the FQDN to communicate with the system that hosts the Paging server.
Service Port	4200	If you must change the default, see Changing the service port for the Paging server on page 519. Port conflicts can cause serious problems within the IC system.
ComHub Host Name	Enter the fully-qualified domain name of the system that hosts the ComHub server of the same Avaya IC domain.	For example, enter TESTBOX.xyzcorp.com.

6. If you change the default service port of 4001 for the Comhub server, perform the following steps:
   a. Right-click a blank space of the **Paging** tab.
   b. Select the box next to **Show Advanced Properties**.
   c. In the **Comhub Port** field, type the service port for the Comhub server.
7. Click **Ok**.

Starting the Web Management servers

Before you configure your media channels, start the IC servers, including the Web Management servers. When you start the Attribute server, the WebACD server starts automatically and starts the next paired WebACD server from the WACD_Cluster.

To start the Web Management servers:

1. In IC Manager, select the server.
2. Right-click the server and select **Start**.

For more information about the correct order for starting and stopping Web Management and other IC servers, see Starting and stopping IC servers on page 107.

Setting startup options for servers in IC Manager

Set the following Web Management servers to autostart:

- Attribute server
- ComHub server
- Paging server
- Workflow server that processes chat contacts

To set startup options for servers in IC Manager:

1. In IC Manager, double-click the server in the **Server** tab.
2. Click the **General** tab.
3. Select the **Auto Start** box.

Configuring Web Management services

This section describes how to install and configure Web Management services for each operating system that IC supports. This section includes the following topics:

- Where to configure Web Management services on page 207
- Hosting multiple Web applications on a system on page 207
- Setting memory allocation for Web Management services on page 207
- Configuring Web Management services on Windows on page 208
- Configuring Internet Information Services on page 213
- Configuring Web Management services on Solaris on page 216

- Configuring Web Management services on AIX on page 222.

Where to configure Web Management services

Configure Web Management services on the following:

- Systems that host Web Management websites
- Systems that host the WebACD servers and Attribute servers to configure database access for:
  - Suggested Response feature of the WebACD server.
  - DataWake recording feature of the Attribute server.

Hosting multiple Web applications on a system

If the IC system includes more than one Web application on the same system as the WebLM, you must configure all of the Web applications on the target system at the same time.

WARNING:
If you do not configure all of the Web applications simultaneously, leave the options for all Web applications on the target system selected when you re-run the Configuration Tool to create new Web applications. If you do not leave the options for the previously created Web applications selected, the Configuration Tool may delete those Web applications.

Setting memory allocation for Web Management services

The Web tab also includes advanced properties for the Java Virtual Machine. Only configure the advanced properties if you expect a high volume of contacts on the website. For more information, see Configuration Tool advanced properties on page 520.

The advanced properties use the following format:

```
-<initial_Java_heap> -<maximum_Java_heap>
```

If you expect a high volume of chat contacts, increase the default settings for the advanced properties. For example, you can use the advanced properties to increase the memory allocations for the website JVM, and ICM JVM should be adjusted upward. For high volumes, configure each of these properties to:

Website JVM Options	`--JvmMs 256 --JvmMx 1024`
	`-Xms128m -Xmx512m`
	`-Xms128m -Xmx512m`

ICM JVM Options	All Platforms: `-Xms128m -Xmx512m`

Configuring Web Management services on Windows

Use these instructions if you plan to host Web Management services on a Windows system.

You do not need to stop the IIS Web server on Windows systems.

To configure Web Management services to run on a Windows system:

1. To start the Configuration Tool, select **Start** > **Programs** > **Avaya Interaction Center** 7.3 > **Configuration Tool**.

   If the Configuration Tool is already open, close and re-open it to ensure that the Configuration Tool includes all system changes, such as new servers.
2. Log in with your IC Manager login ID and password.
3. Click the **Web** tab.
4. Enter the information for the general fields mentioned in the following table:

Field	Description	Sample entry
Tomcat Base Port	The port used to configure the following ports: • Tomcat HTTP ports for Web applications • Tomcat AJP (Web server connector) ports	Default: 9600
IIS Website	The name of the IIS Web server that the Web application uses. **Tip:** For a localized version of IIS, type the localized name for the IIS Web server.	Default website
Web Server Host	The name of the system that hosts the Web server. Do not include the DNS domain.	testbox

Field	Description	Sample entry
DNS Domain	The network (DNS) domain of the system that hosts your Web server. Do not enter an IC domain. **Note:** Verify the default DNS domain carefully to ensure that it is correct.	xyzcorp.com
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: • HTTP port is 80. • HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application on each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: **`http://<server>.<domain>.com:9600/ictest`** **Note:** The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Select this box

5. Enter the information for the Web Management fields mentioned in the following table:

Field	Description	Sample entry
Configure Web Management	Select this box if you want to configure Web Management services on the target system. After you select this box, the Configuration Tool automatically displays the other Web Management fields: • Select the following boxes: – Website – ICM – CIRS – Attribute - DataWake recording (PDM)	Select this box.
Website	Creates the website Web application and performs other tasks that are required to configure a Web Management website on the target system. After you select this box, the Configuration Tool displays the following required fields for the website: • Website Virtual Directory Name • WebACD • Attribute Server	Select this box.
Website Virtual Directory Name	The name of the virtual directory for the website.	website
WebACD	The WebACD server in your IC system. You must create the WebACD server before the Configuration Tool can include the server in the drop-down list. If the list does not include the server, close the Configuration Tool and create the server. For more information, see Creating the WebACD server on page 196.	WebACD_web

Field	Description	Sample entry
Attribute Server	The Attribute server that the DataWake plug-in uses. You must create the Attribute server before the Configuration Tool can include the server in the drop-down list. If the list does not include the server, close the Configuration Tool and create the server. For more information, see Creating the Attribute server on page 200.	Attribute_web
ICM Service	Configures the ICM server and related components on a target system. For more information, see Configuring the ICM server on page 237.	Select this box.
CIRS Service	Configures the CIRS server and related components on a target system. For more information, see Configuring the Central Internet Routing service on page 240. **Important:** Only configure a CIRS server if your IC system includes more than one ICM server.	Select this box.
Attribute - DataWake recording (PDM)	Configures the DataWake recording feature of the Attribute server.	Select this box.
IC Login	Use the website account that you imported into the database with the seed data. If you have not already imported the database, change the default password for the website account. For more information, see *Interaction Center Administration Guide*. **Note:** Do not use the Administrator account for IC Manager or any other account for which the password may change.	website
IC Password	The password used by the IC Login.	website

Field	Description	Sample entry
IC Data Source	The Interaction Center data source that you create with the Interaction Center application for the CallCenterQ database. For more information, see Generating the Interaction Center application on page 151.	interaction_center
Repository Data Source	The Repository data source that you create with the repository application for the IC Repository database. For more information, see Generating the IC Repository application on page 142.	repository
Database Login	Type a DBA login ID for the database server.	*SQL Server*: sa *Oracle*: system
Database Password	The password for the DBA login ID.	admin
SQL Driver (Windows Only)	Select an appropriate ODBC driver.	The drop-down list displays only the ODBC drivers that you installed on the system. This field is available from IC 7.3.3. The options that appear based on the ODBC driver installed on the system are: • SQL Server (Installed with Microsoft Windows server OS) • SQL Server Native Client 10.0 (Installed with SQL Server2008) • SQL Server Native Client 11.0 (Installed with SQL Server2012)
Oracle Home	*Oracle databases only.* The home directory of the Oracle client on the system that hosts the Web Management servers.	*SQL Server*: leave empty *Oracle*: `C:\app\Administrator\product\11.2.0\client_1`

6. Click **Apply Settings**.
7. Click **OK** in the **Success** dialog box.
8. Click **Exit**.
9. To complete the configuration, perform the following steps to ensure that all Web Management services start properly:

a. Open the Windows Services control panel.

b. Start Avaya IC Web Management Service 7.3, as described in Starting and stopping IC services on page 114.

Configuring Internet Information Services

IC installs various ISAPI filters and extensions on the Web server which hosts the website. Avaya develops some of these filters, while the Tomcat Redirector is a third-party ISAPI filter.

Due to the complexities involved, the following outlines the process to add any ISAPI filter/ extension to an IIS 7.x server.

Configuring IIS server for Windows 2008 R2 server

To configure IIS7.x in Windows 2008 R2 server, invoke Server manager -> Roles -> Web Server (IIS) -> Internet Information Services (IIS) Manager.

To add a plugin to IIS7.x using the IIS manager:

1. Allow the plugin to run on the server:
   a. Click the server node, and double-click **ISAPI and CGI restrictions** node on the home page.
   b. Click **Add** in the **Actions** pane.
   c. Add the full path to the plug-in, and enter a description.
   d. Select **Allow extension path to execute** option.
2. Add the plugin as an ISAPI filter on the website:
   a. Click the website where Avaya IC website is deployed. For example, the default website.
   b. In the home page of the website, double-click **ISAPI filters** node.
   c. Click **Add** in the Actions pane.
   d. Type a name for the filter, and add the complete path to the plug-in. This path is the same as that entered in the previous step.
3. Add Handler Mapping for the plug-in on the website:
   a. Click the website where Avaya IC website is deployed. For example, the default website.
   b. In the home page of the website, double-click the **Handler Mappings** node.
   c. Click **Add Script Map** in the **Actions** pane.
   d. In the **Request path** text box, enter the file name of the plug-in. For example, isapi_redirect.dll.

e. Enter the complete path in the **Executable** text box. This is the same as the path given in the previous 2d step.

f. Give a name for the script mapping.

g. Click **Request Restrictions**.

1. In the **Mapping** tab, select the **invoke handler** option.
2. Select the **File or folder** option.
3. In the **Verbs** tab, select the **All verbs** option.
4. In the **Access** tab, select the **Script** option.

4. Add read permissions to the folder where the plugin is installed:

a. The website runs under a certain **Application Pool** in IIS. The identity which the Application Pool runs requires that it have read permission to all folders where plug-ins defined for the website are installed. Unless this is done, the website may not get access to the plug-ins and they may fail to load.

b. 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/set from the dialog thus shown. Take a note of the application pool used.

c. To determine the identity used by the application pool, click the **Application Pool** node. Select the application pool noted in the previous step, and select **Advanced Settings** from the Action panel. The identity of the Application Pool can be read/set using this dialog box. The value in the "Identity" property can either be an account name for example, LocalService, NetworkService, and so on, or can be set as "ApplicationPoolIdentity". If it is an account name, then the specified account needs to have read access to the folders where the plug-ins are installed. In case Identity is set as ApplicationPoolIdentity, then the account IIS AppPool\<application pool name> is used; where <application pool name> is the name of the application pool for example, DefaultAppPool). Whenever an application pool is created, a user with the given format is created, and is used as the default identity for the pool. These users are not visible under Local Users of the system.

d. Once the Application pool identity account is determined, allow read permissions to this account on the folder(s) where the plug-in(s) are installed.

5. Add read/write permissions to folders where plug-ins write logs:

a. Some plug-ins may write logs, and the application pool identity account should have read/write access to these folders. If this is not the case, then the plug-ins may not be able to write logs for troubleshooting.

b. Once the Application pool identity account is determined, allow read/write permissions to this account on the folders where the plug-ins writes logs.

6. Enabling 32-bit applications for the Application pool:

a. As IC plug-ins are 32-bit applications, the Application Pool under which the website runs must be setup to run 32-bit applications, else the plug-ins) do not load, and the system displays an error in the browser when navigating the website.

b. Click the Application Pools node. Select the application pool which services the website which hosts the IC website. For example, DefaultAppPool. Click **Advanced settings** in the **Actions** pane. The system displays a dialog box. In the **General** section, set the "Enable 32-bit Applications" property to true. Click **OK**.

In the above steps, it is easier to manage the system if the same name/description is given when creating the ISAPI/CGI restrictions rule, creating the ISAPI filter, and creating the Handler Mappings.

Configuring the Tomcat Redirector for IIS

When you host a customer website on IIS, a third-party ISAPI filter is used to redirect requests for the IC website to the Tomcat Server that hosts Web Management Service. This filter (isapi_redirect.dll) is also known as Tomcat Redirector.

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. Additionally, when the Tomcat Redirector is installed on a customer facing website, the actual Tomcat server typically resides in the local LAN across a firewall. Firewall related configurations are provided to minimize issues due to connection drops due to firewall timeouts.

1. The application pool, under which the website runs, must have worker recycling disabled.
   a. 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.
   b. Click the **Application Pool Node**. Select the application pool noted in the previous step, and click **Advanced Settings** from the Action panel.
   c. Make the following changes to the settings:
      - Set **Limit Interval** under CPU to 0.
      - Set **Idle Time-out** under Process Model to 0.
      - Set **Regular Time Interval** under Recycling to 0.
      - Set **Disable Recycling for configuration changes** under Recycling to true.
2. Modify the Firewall related configurations:

a. The problem with idle connections comes from firewalls that are often deployed between the web server layer and the backend. Depending on their configuration, they silently drop connections from their status table if they are idle for a time that is longer than the firewall timeout value.

b. From the point of view of Tomcat Redirector and the Tomcat server, the other side does not answer any traffic. Since TCP is a reliable protocol, it detects the missing TCP ACKs and tries to resend the packets for a relatively long time, typically for several minutes. Therefore, you must always use `connection_pool_timeout` and `connection_pool_minsize` on the JK side and `keepAliveTimeout` on the Tomcat side to prevent idle connection drop.

c. The recommend 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 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. For details on Workers.properties deprecated directives, see the Apache website. However, deprecated directives are applicable to users who are migrating from IC 7.x to IC 7.3.

Configuring Web Management services on Solaris

Use these instructions if you plan to host Web Management services on a system with Solaris operating system.

Important:

To configure Web Management services on Solaris, log in as a user with write permissions on the Web server directories and the IC installation directories. The root user usually has these write permissions.

To configure Web Management services to run on a Solaris system:

1. Stop the Oracle iPlanet server that hosts the website application, as described in Starting and stopping Oracle iPlanet Web server on page 116.
2. If the Configuration Tool is already open, close it to ensure that the Configuration Tool includes all system changes, such as new servers.
3. Start the Configuration Tool:
   a. Navigate to *IC_INSTALL_DIR*/IC73/bin
   b. Run **./configure**

4. Log in with your IC Manager login ID and password.
5. Click the **Web** tab.
6. Enter the information for the general fields mentioned in the following table:

Field	Description	Sample entry
Tomcat Base Port	The port used to configure the following ports: • Tomcat HTTP ports for Web applications • Tomcat AJP (Web server connector) ports	Default: 9600
Web Server Home	The installation path for the iPlanet Web Server that hosts the Web application.	/opt/oracle/ websever7.0
Web Server Name	The root name of the server as found in the iPlanet Server home directory. Note: Do not include https- in the Web server name.	testbox.xyzcorp.com
Web Server Host	The name of the system that hosts the Web server. Do not include the DNS domain.	testbox
DNS Domain	The network (DNS) domain of the system that hosts your Web server. Do not enter an IC domain. **Note:** Verify the default DNS domain carefully.	xyzcorp.com
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: • HTTP port is 80. • HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80
Deploy iPlanet Configuration	If this box is selected, the configtool pulls and deploys the configuration changes of server instance to the config store.	Select this box if you would like the configtool to pull and deploy configuration.
iPlanet Webserver Config	iPlanet configuration used for website configuration.	
iPlanet Webserver Node	A Node is a network resource, such as a server or a host on which Admin server is installed	Hostname

Field	Description	Sample entry
iPlanet Webserver Admin Login	An Admin login given at the time of iplanet installation.	Default is "admin"
iPlanet Webserver Admin Password	Admin password given at the time of iplanet installation.	
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application on each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: http://<server>.<domain>.com:9600/ictest Note: The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Select this box.

Note:

You can pull the configuration changes manually to the config store through the following steps:

From the Command Line:

a. Start the Web Server 7.0 Administration Server. See the *Interaction Center Administration Guide*.

b. For pulling the changes back to the Administration Server repository, execute the following command.

```
wadm> pull-config --user=admin --config=CONFIG_NAME
```

From the Administrator Console:

a. Start the Administrator Console (for example, https:// support.xyzcorp.com:8989/) where 8989 is the default port on which administrative server is running.

b. On the admin console, select the Configuration and virtual server on which the website is deployed.

c. Select Edit Virtual server.

d. On the right top corner, a link with message "Instance Configuration Modified" is displayed. click the link and choose 'pull and deploy configuration' and click **OK**.

7. Enter the information for the **Web Management** fields mentioned in the following table:

Field	Description	Sample entry
Configure Web Management	Select this box if you want to configure Web Management services on a target system. After you select this box, the Configuration Tool automatically: • Displays the other Web Management fields • Selects the following boxes: – Website – ICM – CIRS – Attribute - DataWake recording (PDM)	Select the box
Website	Creates the Website Web application and performs other tasks that are required to configure a Web Management website on a target system. After you select this box, the Configuration Tool displays the following required fields for the website: • Website Virtual Directory Name • WebACD • Attribute Server	Select the box
Website Virtual Directory Name	The name of the virtual directory for the website.	website
WebACD	The WebACD server in your IC system. You must create the WebACD server before the Configuration Tool can include the server in the drop-down list. If the list does not include the server, close the Configuration Tool and create the server. For more information, see Creating the WebACD server on page 196.	WebACD_web

Field	Description	Sample entry
Attribute Server	The Attribute server that the DataWake plug-in uses. You must create the Attribute server before the Configuration Tool can include the server in the drop-down list. If the list does not include the server, close the Configuration Tool and create the server. For more information, see Creating the Attribute server on page 200.	Attribute_web
ICM Service	Configures the ICM server and related components on a target system. For more information, see Configuring the ICM server on page 237.	Select the box
CIRS Service	Configures the CIRS server and related components on a target system. For more information, see Configuring the Central Internet Routing service on page 240. **Important:** You must configure a CIRS server only if your IC system includes more than one ICM server.	Select the box
Attribute - DataWake recording (PDM)	Configures the DataWake recording feature of the Attribute server.	Select the box
IC Login	Use the website account that you imported into the database with the seed data. If you have not already imported the website account, change the default password for this account. For more information, see *Interaction Center Administration Guide*. **Note:** Do not use the Administrator account for IC Manager or any other account for which the password may change.	website
IC Password	The password used by the IC Login.	website

Field	Description	Sample entry
IC Data Source	The Interaction Center data source that you create with the Interaction Center application for the CallCenterQ database. For more information, see Generating the Interaction Center application on page 151.	interaction_center
Repository Data Source	The Repository data source that you create with the repository application for the IC Repository database. For more information, see Generating the Interaction Center application on page 151.	repository
Database Login	Type a DBA login ID for the database server. **Note:** Do not use the DBA login for a database client on a DB2 database.	*Oracle*: system
Database Password	The password for the DBA login ID.	admin
Database Host	The host name of the system that hosts your database server.	testbox.xyzcorp.com
Oracle SID	The Oracle SID of your database. **Note:** The Oracle SID field is case-sensitive.	icutf8db

8. Click **Apply Settings**.
9. Click **Ok** in the **Success** dialog box.
10. Click **Exit**.
11. To complete the configuration, perform the following steps to ensure that all Web Management services start properly:
    a. In the iPlanet Server installation directory:
       - Open the admin-server directory.
       - If the directory includes a file called start-ICEnv.backup, execute the following command to rename the file:

         ```
         mv start-ICEnv.backup oldstart-ICEnv
         ```

    b. Start the Oracle iPlanet server that hosts the website application, as described in Starting and stopping Oracle iPlanet Web server on page 116.

c. Navigate to the *IC_INSTALL_DIR*/IC73/bin directory and use the following script to start Tomcat:

nohup ./ictomcat.sh start website

Important:
For Solaris only, the Configuration Tool changes the ownership of the implementation file (vesp.imp) and the interface file (vespidl.pk) to root. If you do not want to run IC as root, you must change the ownership of these files as described in Changing the ownership for IC on page 49.

Configuring Web Management services on AIX

Use these instructions if you plan to host Web Management services on an AIX system.

Important:
To configure Web Management services on AIX, log in as a user with write permissions on the Web server directories and the IC installation directories. The root user usually has these write permissions.

To configure Web Management services to run on an AIX system:

1. Stop the IBM HTTP Server that hosts the Website application, as described in Starting and stopping IBM http Web server on page 119.
2. If the Configuration Tool is already open, close it to ensure that the Configuration Tool includes all system changes, such as new servers.
3. Start the Configuration Tool:
   a. Navigate to *IC_INSTALL_DIR*/IC73/bin
   b. Run **./configure**
4. Log in with your IC Manager login ID and password.
5. Click the **Web** tab.
6. Enter the information for the general fields mentioned in the following table.

Field	Description	Sample entry
Tomcat Base Port	The port used to configure the following ports: • Tomcat HTTP ports for Web applications • Tomcat AJP (Web server connector) ports	Default: 9600
Web Server Home	The installation path for the IBM HTTP server instance that hosts the Web application.	/usr/HTTPServer

Field	Description	Sample entry
Web Server Host	The name of the system that hosts the Web server. Do not include the DNS domain.	testbox
DNS Domain	The network (DNS) domain of the system that hosts your Web server. Do not enter an IC domain. **Note:** Verify the default DNS domain carefully to ensure that it is correct.	xyzcorp.com
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: • HTTP port is 80. • HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application on each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: `http://<server>.<domain>.com:9600/ictest` **Note:** The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Select the box

7. Enter the information for the Web Management fields mentioned in the following table:

Field	Description	Sample entry
Configure Web Management	Select this box if you want to configure Web Management services on a target system. After you select this box, the Configuration Tool automatically: • Displays the other Web Management fields • Select the following boxes: – Website – ICM – CIRS – Attribute - DataWake recording (PDM)	Select the box
Website	Creates the Website Web application and performs other tasks that are required to configure a Web Management Website on a target system. After you select this box, the Configuration Tool displays the following required fields for the Website: • Website Virtual Directory Name • WebACD • Attribute Server	Select the box
Website Virtual Directory Name	The name of the virtual directory for the Website.	website
WebACD	The WebACD server in your IC system. You must create the WebACD server before the Configuration Tool can include the server in the drop-down list. If the list does not include the server, close the Configuration Tool and create the server. For more information, see Creating the WebACD server on page 196.	WebACD_web
Attribute Server	The Attribute server that the DataWake plug-in uses. You must create the Attribute server before the Configuration Tool can include the server in the drop-down list. If the list does not include the server, close the Configuration Tool and create the server. For more information, see Creating the Attribute server on page 200.	Attribute_web

Field	Description	Sample entry
ICM Service	Configures the ICM server and related components on a target system. For more information, see Configuring the ICM server on page 237.	Select the box
CIRS Service	Configures the CIRS server and related components on a target system. For more information, see Configuring the Central Internet Routing service on page 240. **Important:** Only configure a CIRS server if your IC system includes more than one ICM server.	Select the box
Attribute - DataWake recording (PDM)	Configures the DataWake recording feature of the Attribute server.	Select the box
IC Login	Use the website account that you import into the database with the seed data. If you have not already imported the website account, change the default password for this account. For more information, see *Interaction Center Administration Guide*. **Note:** Do not use the Administrator account for IC Manager or any other account for which the password may change.	website
IC Password	The password used by the IC Login.	website
IC Data Source	The IC data source that you create with the IC application for the CallCenterQ database. For more information, see Generating the Interaction Center application on page 151.	interaction_center
Repository Data Source	The Repository data source that you create with the repository application for the IC Repository database. For more information, see Generating the IC Repository application on page 142.	repository
Database Login	Type a DBA login ID for the database server. **Note:** Do not use the DBA login for a database client on a DB2 database.	*DB2*: db2inst1

Field	Description	Sample entry
Database Password	The password for the DBA login ID.	admin
Database Host	The host name of the system that hosts your database server.	testbox.xyzcorp.com
DB2 Port	The port that the target system uses to communicate with the DB2 database.	Default: 50,000

8. Click **Apply Settings**.
9. Click **Ok** in the **Success** dialog box.
10. Click **Exit**.
11. To complete the configuration, perform the following steps to ensure that all Web Management services start properly:
    a. Start the IBM HTTP Server that hosts the website application as described in Starting and stopping IBM http Web server on page 119.
    b. Navigate to the *IC_INSTALL_DIR*/IC73/bin directory.
    c. Use the following script to start Tomcat:

       nohup ./ictomcat.sh start website

Important:
For AIX only, the Configuration Tool changes the ownership of the implementation file (vesp.imp) and the interface file (vespidl.pk) to root. If you do not want to run IC as root, you must change the ownership of these files as described in Changing the ownership for IC on page 49.

Integrating Web Management Administration

Web Management Administration is a set of Web pages that you use to administer and configure Web Management and Email Management. You can open Web Management Administration from IC Manager. Before you use Web Management Administration, you must integrate Web Management Administration with IC Manager.

Note:
Complete only those properties listed in this section to integrate Web Management administration. You do not need to complete the other properties available in the System/Configuration list.

This section includes the following topics:

- Integrating Web Management Administration with IC Manager on page 227
- Setting the ServerName property - AIX only on page 228

Integrating Web Management Administration with IC Manager

To integrate Web Management Administration with IC Manager:

1. In IC Manager, select **Tools** > **Groups**.
2. Click the **Properties** tab.
3. In the left pane, select the **IC** node.
4. In the **Sections** list, select **System/Configuration**.
5. From the list of properties, double-click the **Value** column next to ChatLoginServer and enter the information for the following fields:
   a. In the **Property Value** field, type the fully-qualified domain name of a system that hosts the Tomcat server for the Web Management Administration website. For example, type support.xyzcorp.com.
   b. Click **Ok**.
6. From the list of properties, double-click the **Value** column next to ChatLoginServerWebsite and enter the information for the following fields:
   a. Type the name of the Tomcat web application for the Web Management Administration website.

      This is the name that you specified when you configured the website Tomcat application in Configuring Web Management services on page 206. The Web Management Administration Website must be on a system that you specified for the ChatLoginServer property.
   b. Click **Ok**.

7. If you serve your Web Management Administration pages from a secure web server, you must also modify the properties shown in the following table:

Property	Recommended entry	Notes
ChatLoginServerProtocol	Type the protocol that your Web server uses.	For secure server protocol, type **https**. For non-secure server protocol, type **http**.
ChatLoginServerPort	Type the following ports: • HTTP - 80 • HTTPS - 443	Do not change the default port.

8. Click **Ok**.
9. Exit and restart IC Manager.

Setting the ServerName property - AIX only

The default installation of the IBM http server does not include the fully qualified domain name for the ServerName property in the httpd.conf file. If the ServerName property is incorrect, the Web Management Administration pages can loop indefinitely on the opening page.

To set the ServerName property:

1. In a text editor, open the `.../HTTPServer/conf/httpd.conf` file.
2. Search for the `ServerName` entry and ensure that the value includes the fully qualified domain name of the server.
3. Save the file.
4. Restart the IBM http server, as described in Starting and stopping IBM http Web server on page 119.

Configuring a Workflow server for Web Management

To configure the Workflow server for Web Management, perform the steps in the following topics:

1. Creating a Workflow server for Web Management on page 229
2. Creating the chat channel for the Workflow server on page 230

If your IC system includes multiple Workflow servers, perform these steps on each Workflow server that processes chat contacts.

Creating a Workflow server for Web Management

These instructions provide information only about those parameters you need to set when you create a Workflow server to handle chat contacts. If you have configured two WebACD servers, create two Workflow servers for Web Management. For example, if `Web` and `Web2` are two domains where you have configured `WebACD1` server and `WebACD2` server respectively. Then, you must configure the WebManagement Workflow servers in both `Web` and `Web2` domain.

For more information about other parameters in the Workflow server, see Configuring multiple Workflow servers on page 94 and *Interaction Center Administration Guide*.

CAUTION:
If you do not configure the Workflow server with synchronous startup flows, the Qualify Chat workflow cannot resolve the pkey of the queue where a contact must be routed. If this occurs, IC cannot route chat contacts.

To create a Workflow server for Web Management:

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **Workflow**.
3. Click **OK**.
4. Click the **General** tab, and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	Workflow_<*domain*>	Include the domain in the server name to identify the server.

Field	Recommended entry	Notes
Domain	Select the IC domain for the server from the drop-down list.	For example, you can select `Web` or `Web2` to use the preconfigured domain for Web Management.
Host	Select the IP address of the system from the drop-down list, or type the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. Click the **Workflow** tab.
6. From the **IC Data Source** drop-down list, select the Interaction Center data source.

   The default name for this data source is interaction_center. This is the data source that you created in Generating the Interaction Center application on page 151.
7. Select **Synchronous Startup Flows.**
8. If the following rows do not exist, add them to the Synchronous Startup Flows:
   a. Click **New**.
   b. In the new row, type **`web_routing.update_qw_cache`**
   c. Click **OK**.
9. Continue with Creating the chat channel for the Workflow server on page 230.

Creating the chat channel for the Workflow server

To create the chat channel for the Workflow server:

1. In the Server Editor for the Workflow server, click the **Channels** tab.
2. Select **New Channel**.
3. In the **Channel Editor** dialog box:

a. Enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Global	Do not select this field.	Do not select this field to create a create a channel for a specific server or media such as Chat.
By Server	• Do not select this field if you want this channel to handle events from all servers of the type that you select from the **Service** drop-down list. • Select this field if you want this channel to handle events from only one specific server that you select from the **Service** drop-down list.	If you select this field, and you need this Workflow server to communicate with more than one server, you must create another channel for that server. **Warning:** If you select this field and the WebACD server is named "WACD", the Workflow server cannot communicate with the WebACD server.
Channel Range	No entry necessary.	Completed by IC Manager
Service	Select **WACD** or the WebACD server from the drop-down list.	Whether you can select a server or a type of server depends on whether or not you selected the **By Server** field.
Criteria	Type **media=chat**	The field value is case sensitive. You must specify the value as mentioned.

b. Click **OK**.

4. Select the channel that you created in the previous step.
5. Click **New Association**.
6. In the **Channel Association** dialog box, enter the information for the fields mentioned in the following table and click **Ok**.

Field	Recommended entry
Channel Range	Completed by IC Manager
Service Range	Completed by IC Manager

Field	Recommended entry
Event	WACD.QualifyChat **Note:** This field is case-sensitive.
Flow	***<flow_project>.<flow_name>*** For example, to use the sample workflow, type **wacd.qualifychat**

7. Click **OK**.
8. In the **Server** tab of IC Manager, select the Workflow server that handles chat contacts.
9. Right-click the Workflow server and select **Start**.

Using workflows for Web Management

You can use the sample workflows to configure and test your Web Management servers. When you move into production, modify the sample workflows to meet your system needs and configuration. For more information, see *Avaya IC Media Workflow Reference*.

Note:
If you add a queue to route chat contacts, you must re-run the update_qw_cache workflow in the Web_Routing project. If you do not want to stop and start the Workflow server that processes chat contacts, select **Run Flows** on the General tab of the Workflow server.

This section includes the following topics:

- Workflows required by Web Management on page 232
- Reloading the customer management workflows on page 233

Workflows required by Web Management

Web Management requires the following sample and system workflows:

- Qualify Chat workflow in the WACD project.
- All workflows in the WebRouting project.
- All workflows in the WebCenter project.

The IC seed data includes compiled sample workflows for these projects. When you create the CCQ database, you import the compiled workflows with the seed data and store them in the database.

For a complete list of the workflows in these projects, including the directories where IC installs the workflows, see *Avaya IC Workflow Designer User Guide*.

Important:
Make sure that no workflows use a formatted telephone number to look up customer records. For example, confirm that your Qualify Chat workflow does not use a formatted telephone number in the Customer Lookup block.

Reloading the customer management workflows

The customer management workflows in the WebCenter project require file-based Avaya IC Scripts. By default, the `include` property contains the names of the required file-based IC Scripts.

Before you compile the workflows in the WebCenter project, add the following Avaya IC Script directory to the project:

IC_INSTALL_DIR\IC73\design\IC\Flows\Avaya\WebCenter

To add the Avaya IC Script directory:

1. With the project open in Workflow Designer, select **Project** > **Settings**.
2. In the **Directories** tab of the **Project Settings** dialog box, select **New Folder**.
3. In the **Open** dialog box:
   a. Navigate to the following IC Script folder:

      IC_INSTALL_DIR\IC73\design\IC\Flows\Avaya\WebCenter

   b. Click **Ok** to add the Avaya IC Script folder to the **Directories** tab.
4. If you have not already done so, in the **Project Settings** dialog box:
   a. Click the **Database** tab.
   b. Verify that the **IC Data Source** field includes the name of the Interaction Center data source.
   c. In the **Login Id** field, enter an administrative account for IC.
   d. In the **Password** field, enter the password for the administrative account.
5. In the **Project Settings** dialog box, click **Ok**.

   You can now compile and load the customer management workflows.

Configuring routing hints for the Qualify Chat workflow

The Fetch Routing Hints (chat) block in the Qualify Chat workflow uses the routing hints in the RoutingHint table of the Directory server to route incoming chat contacts. The following table shows the routing hints used in the sample Qualify Chat workflow:

Category	Sample routing hint values
language	This category requires ISO-639-1 values, such as: • en • sp • fr • de • zh
intent	• sales • support

To route chat contacts with the sample Qualify chat workflow, create these hints, then assign them to the default chat queue.

Important:
The routing hints must be in lower case. Do not use mixed upper and lower case in your routing hints. If the routing hint is not in all lower case, the workflow cannot locate the routing hint, and Avaya IC cannot route the contact correctly.

To configure routing hints, perform the steps in the following topics:

1. Creating routing hints on page 234.
2. Associating routing hints with Web Self-Service documents on page 236.

Creating routing hints

Use the Configuration tab of IC Manager to create routing hints and add them to the RoutingHint table. The Qualify Chat workflow uses hints from the RoutingHint table to route incoming chat contacts.

Each row in the routing hint table contains the following:

- A routing hint.
- The IDs of the queues where contacts that match the routing hint should be routed.

Tip:
The default chat queue is DefaultChatQueue@DefaultTenant. You can create and use additional chat queues for routing chat contacts. For more information, see *Interaction Center Administration Guide*.

To create routing hints:

1. In IC Manager, click the **Configuration** tab.
2. In the left pane, select **Tables** > **Workflow** > **RoutingHint**.
3. Click **New**.
4. In the right pane, enter the information for the fields mentioned in the following table:

Parameter	Recommended entry	Description
Routing Hint	Type a routing hint.	For the sample Qualify Chat workflow, enter a value for the language or intent category. For language, type a value such as: – en – sp – fr – de – zh For intent, type a value such as: – sales – support The routing hint must be a text string in all lower case. The text string cannot contain any special characters.
Chat Queue ID	Type `DefaultChatQueue@DefaultTenant`.	DefaultChatQueue@DefaultTenant is the default chat queue. For more information about chat queues, see *Interaction Center Administration Guide*.
Category/ Qualifier	Leave this field blank.	Used only for routing hints for chat contacts in Business Advocate.
Tenant	Select `DefaultTenant` from the queue from the drop-down list.	Select the tenant used by the queue. For the DefaultChatQueue, select DefaultTenant to ensure that the routing hint uses the correct queue.

5. Click **Ok**.

   Repeat Steps 3 through 6 to create the second routing hint.

6. Select **Manager** > **Refresh**.

Associating routing hints with Web Self-Service documents

After you add the routing hints to the Directory server tables, you can associate the routing hints with documents in the Web Self-Service database.

When a customer requests a chat contact with an agent, Web Management records the last document that the customer viewed on the website. If that document has an associated routing hint, the Qualify Chat workflow uses that routing hint to determine the correct queue for the chat contact.

You must create at least one document for that database to fully test the Qualify Chat workflow. For more information about the Web Self-Service database, see *Interaction Center Administration Guide*.

To associate routing hints with Web Self-Service documents:

1. In IC Manager, select **Services** > **Web Response Unit**.
2. In the left pane, select **Web Self-Service Console**.
3. On the Web Self-Service Console page:
   a. Select a tenant from the drop-down list.
   b. In the left pane, select **Manage FAQ**.
4. On the Manage FAQ page:
   a. Select the document in the list of documents.
   b. Click **Update**.
5. In the document, scroll down to the **Routing Attributes** section.
6. Select one routing hint from the **Routing Hint** drop-down lists.
7. Click **Update**.

Configuring the ICM server

The ICM server is a service that hosts text conference for Web Management. The ICM server does not run in IC Manager. For information about how to stop and restart the ICM server, see Starting and stopping IC services on page 114.

Important:
The steps in *Configuring the ICM server* are optional. Do not perform these steps if the ICM server requires only the default functionality. For example, perform these steps if you want to increase the logging level from the default logging level of "1".

Do not enter a value or change the default values in the fields available through **Advanced Properties** unless a property needs to be explicitly changed from the default value calculated by the ICM server during its initialization. Most IC systems do not require setting any of the advanced properties. For more information about the advanced properties, see *Interaction Center Administration Guide*.

To configure the ICM Server:

1. In IC Manager, click the **Configuration** tab.
2. From the **Tables** list in left pane, select **Chat** > **ICM**.
3. Click **New**.
4. In the right pane, type a name for the ICM server in the **Global ICM Name** field.

   If your Avaya IC system includes multiple ICM servers, type the name that allows you to easily identify the ICM server. For example, for an ICM server on the TESTBOX system, type **`icm_TESTBOX`**.

   Important:
   The ICM server name is case-sensitive.

   The ICM server uses the global name to determine which ICM record to read for configuration. The global name in this field must match the **`dsObject`** parameter in the following file on the system that hosts the ICM server:
   `IC_INSTALL_DIR``/IC73/etc/systemParms.txt`

5. In the right pane, review the fields as shown in the following table:

Note:

Do not enter a value or change a default value in these fields unless a property needs to be explicitly changed from the default value calculated by the ICM server during initialization. Most IC systems do not require changing any of these fields. When you configure multiple ICMs, you must also configure multiple websites. CIRS does the load balancing across ICMs and uses the corresponding website when performing load balancing. Therefore, if CIRS and multiple ICMs are configured but the corresponding websites are not, CIRS fails to perform load balancing.

Parameter	Description
ICM Active	External clients use this parameter to determine which ICMs to use.
Enable Emoticons	Select this check box to enable emoticons in the Chat application. With chat message, you can send emoticons to the client. For more information, see *Avaya Agent Web Client Online Help*.
ICM Server Name	The fully-qualified domain name of the system that hosts the ICM server.
SMTP Host	The fully-qualified domain name of the system that hosts the SMTP server. For example, **`SMTPSVR.xyzcorp.com`**. The SMTP hostname mentioned in this field is used only when the system does not have any email accounts configured in the IC manager. In this case, the 'From' address in the chat transcript is 'support@<hostname>'. If email accounts are configured in the IC manager, the SMTP hostname specified in the default email account configuration is used. The first email account configured in the IC manager is the default email account. If this account is disabled, the account configured next is treated as the default account. This process continues till an email account that is not disabled is found.
Chat Transcript Directory	The directory where IC stores the chat transcripts. The default directory is *`IC_INSTALL_DIR`*`\IC73\comp\icm\transcript`
Style Sheet Directory	The directory where IC stores the style sheets used to format emails that include chat transcripts. If you use the default installation directory, IC Manager automatically enters the following directory: `../comp/icm/transcriptxsl`

Parameter	Description
CIRS Host	The name of the system that hosts the CIRS server used for load balancing.
ICM Property Management Debug Level	A number from 0 to 4 that represents the debug level for ICM components. Level 0 provides no debugging information in the logs, and level 4 provides full debugging information.
ICM Toolkit Debug Level	A number from 0 to 4 that represents the debug level for ICM toolkit components. Level 0 provides no debugging information in the logs, and level 4 provides full debugging information.
ICM Debug Level	A number from 0 to 4 that represents the debug level for the ICM server. Level 0 provides no debugging information in the logs, and level 4 provides full debugging information.

6. Click **Ok**.
7. Restart the ICM server.

Configuring IIS server for ICM support

Perform the following steps on the system where the ICM server is installed:

Note:
By default, security settings on Windows 2008 R2 Server allow access only to files with certain predefined extensions, such as .html, .xml, .jpg, and so on. To allow client applications to download .ini files, you need to configure your system using the IIS Manager as given below.

1. Stop the Tomcat server, the ICM server, and Website, if already running.
2. Delete all the files and subdirectories in the following directory:

   `.../IC73/tomcat/work/Catalina/localhost/website/org/apache/jsp/public_`

   If no files or directories are present in the `public_` directory, proceed to the next step.
3. Start the IIS Admin tool by following the steps given below:
   a. Open the IIS manager.
   b. Select the website which hosts the IC website. For example, the default website.
   c. On the home page, double-click **Mime Types**.
   d. Click **Add** in the Actions pane.
   e. In the **MIME Type** dialog box,

- Type `.ini` in the **Associated extension** text box.
- Type `Text/Plain` in the **Content type (MIME)** text box.

f. Click **OK** in the **MIME Type** dialog box.

g. Click **OK**.

h. Click **Apply** and then click **OK**.

4. Start the Tomcat server, the ICM server, and website.

Configuring the Central Internet Routing service

If your IC system includes multiple ICM servers, you must configure a Central Internet Routing service (CIRS server) to balance the load between the ICM servers. Repeat the following steps for each CIRS server in your IC system.

The CIRS server does not run in IC Manager. For information about how to stop and restart the CIRS server, see Starting and stopping IC services on page 114.

Important:
The steps in *Configuring the Central Internet Routing service* are optional. Do not perform these steps if the CIRS server requires only the default functionality. For example, perform these steps if you want to increase the logging level from the default logging level of "1".

Do not enter a value or change the default values in the fields available through **Advanced Properties** unless a property needs to be explicitly changed from the default value calculated by the CIRS server during its initialization. Most IC systems do not require setting any of the advanced properties. For more information about the advanced properties, see *Interaction Center Administration Guide*.

To configure the CIRS server:

1. In IC Manager, click the **Configuration** tab.
2. From the **Tables** list in left pane, select **Chat** > **CIRS**.
3. Click **New**.

4. In the right pane, type a name for the CIRS server in the **Global CIRS Name** field.

   The CIRS server name is case-sensitive.

   If your Avaya IC system includes multiple CIRS servers, type a name that allows you to easily identify this CIRS server. For example, for a CIRS server on the TESTBOX system, type **`cirs_TESTBOX`**.

   The CIRS server uses the global name to determine which CIRS record to read for configuration. The global name in this field must match the **`dsObjectName`** parameter in the following file on the system that hosts the CIRS server:
   `IC_INSTALL_DIR``/IC73/etc/cirsSystemParms.txt`

5. In the right pane, review the fields as shown in the following table:

Note:
Do not enter a value or change the default values in these fields unless a property needs to be explicitly changed from the default value calculated by the CIRS server during its initialization. Most IC systems do not require changing any of these fields.

Parameter	Description
CIRS Active	External clients use this parameter to determine which ICMs to use. This box must be selected for the CIRS server to function.
IC Site	Automatically lists all sites in your IC system. This field contains the site where this CIRS server is located.

6. Click **Ok**.
7. Restart the CIRS server.

Configuring the Website

Before you configure the website, create the website application in the Configuration Tool. For more information, see Configuring Web Management services on page 206.

If you are configuring a localized version, you can specify a supported language for the website. For more information, see Configuring the website for supported languages on page 509.

Important:
The steps in *Configuring the Website* are optional. Do not perform these steps if the website requires only the default functionality. For example, perform these steps to create a separate administration website and to disable access to the administration pages on the customer website.

Do not enter a value or change the default values in the fields available through **Advanced Properties** unless a property needs to be explicitly changed from the default value calculated by the Website during its initialization. Most IC systems do not require setting any of the advanced properties. For more information about the advanced properties, see *Interaction Center Administration Guide*.

Note:

For handling large number of chat requests, configure the Website on a separate system and IIS Webserver to be configured on a separate system. For more information, see Configuring the IIS server on a separate system on page 244.

You can install the primary and the secondary websites on the primary and secondary WebACD servers. You must adhere to the following rules while configuring the Webservers, such as IIS, Oracle iPlanet, and Apache.

- Setup the Webserver either on the primary or the secondary website system. If the Webserver is setup on both the systems, the WebAdmin plug-in on both these systems redirects the request to each other, which results in the WebACD page not being displayed.

  In this configuration, two systems are used and the Webserver from either the primary or the secondary website system can be used to host the website.

- Alternatively, you can setup a third system for the Webserver and install the primary website and WebACD on one system and secondary website and WebACD on the other system.

To configure the website:

1. In IC Manager, click the **Configuration** tab.
2. From the **Tables** list in the left pane, select **Website** > **Website Context Configuration**.
3. Click **New**.
4. In the right pane, type a name for the website in the **Global Name** field.

   The website name is case-sensitive.

   Type a name that allows you to easily identify the website. For example, for a website on the TESTBOX system, type **`website_TESTBOX`**.

   The website uses this parameter to determine which website context record to read. This value must match the **`dsObject`** parameter in the following file on a system that hosts the website:
   IC_INSTALL_DIR\IC73\comp\website\WEB-INF\web.xml
5. In the right pane, review the fields as shown in the following table:

Note:

Do not enter a value or change the default values in these fields unless a property needs to be explicitly changed from the default value calculated by the website during its initialization. Most IC systems do not require changing any of these fields.

Parameter	Description
Context Active	External clients use this parameter to determine which website context to use. This box must be selected for the website to function.
CIRS Name	This is the CIRS server to which the ICM CIRS servlet connects to perform load-balancing for chat contacts.
Website Debug Level	A number from 0 to 4 that represents the debug level for the website. Level 0 provides no debugging information in the logs, and level 4 provides full debugging information.
Default hostname for context	The name of the system that hosts the website. Used by external clients to determine the location of your customer-facing website. If you enter a value in this field, Web Management uses this as the default ***system_name*** in the URL for the customer-facing Website. If you leave this field blank, Web Management uses the value that you use in the URL when you access the customer-facing website for the first time. For example, if you use localhost in the URL the first time, the URL is **http://localhost/website/public**.
IC Site	This property is not currently used.
Servlet context name	The name of your website servlet. For example, **website**. This is the web application name in the Tomcat server. Used by external clients to determine website context name. This value is part of the URL used to access the customer-facing website. For example, if you enter support for a customer support website, the URL is: **http://<*hostname*>/support/public**
Default internet protocol	Either HTTP or HTTPS protocol. Used by external clients to determine website protocol.
Default port for context	This is the HTTP connection port that the website uses. The defaults are: • 80 for HTTP • 443 for HTTPS

Comments on this document? infodev@avaya.com

6. Click **Ok**.
7. Restart the Tomcat server that hosts the Website, as shown in the following table:

Operating system	Step
Windows	From the Services Control Panel, restart the Tomcat server.
Solaris	Run the following command: **nohup ./ictomcat.sh start**
AIX	Run the following command: **nohup ./ictomcat.sh start**

Configuring the IIS server on a separate system

To increase the security of the system, and to expose only the required components to the Internet, it is useful to have the IIS on a publicly accessible system, while keeping the rest of the website application hosted on Tomcat behind the company firewall.

Scenario:

System 1: IIS server which hosts the Tomcat redirector. This is the internet facing system.

System 2: AIC Public Website (Tomcat)

Note:

After you configure IIS according to this scenario, you must use the URL of the System 1 for accessing the IC Website.

For example: `http://<IP address of System 1>/website/public/account.jsp`.

To configure IIS server on System 1

1. Install the Web Server Role. Refer to IC Installation Planning and Prerequisites guide. A default website is provided when the Role is installed.
2. Using IIS Manager, create a new site if required, else use the “Default website” to install the redirector. Note the physical path of the site.
3. Add a new application to the website, with the name “aicjakarta”. Note the physical path to the application ‘root’. This is the physical path where the redirector binary is installed. Refer to this location as the “aicjakarta path”.
4. From the `IC_INSTALL_DIR\IC73\tomcat\modules` directory on System 2, copy the following files to “aicjakarta path” on System 1.
   - isapi_redirect.dll

- isapi_redirect.properties

5. Edit the `isapi_redirect.properties` file as mentioned below:
   1. Replace the directory path mentioned for `log_file`, `worker_file`, `worker_mount_file` with `C:\IIS`.

      For example, replace, `log_file=IC_INSTALL_DIR\IC73\tomcat\logs\iis_redirect.log`. with `log_file=<aicjakarta path>\iis_redirect.log`.
6. From the *`IC_INSTALL_DIR`*`\IC73\tomcat\conf` directory on System 2, copy the following files into the aicjakarta path on System 1.
   - workers.properties
   - uriworkermap.properties
7. Edit the `workers.properties` file.
8. Replace the `localhost` value of all the host properties with the IP address of System 2.

   For example, replace `worker.website_ajp13.host=localhost` with `worker.website_ajp13.host=<IP Address of System 2>`.
9. Add the Tomcat redirector plugin to the site where the application “aicjakarta” has been created. Details regarding the steps to install a plugin to IIS are available at Configuring IIS server for Windows 2008 R2 server on page 213. The Tomcat redirector binary is named isapi_redirect.dll, which you placed in the “aicjakarta path” in step 4.
10. Restart the IIS server.

Note:

To access the IC website pages, you must use the complete URL including the file name. For example, `http://<IP address of System 1>/website/public/account.jsp`.

To reduce the possibility of running out of disk space, you can limit the size of the ISAPI filter log by setting the following properties:

a. Open the file isapi_redirect.properties located at the aicjakarta path. For example, D:\Avaya\tomcat_redirect\.

b. Add the following property:

   # Rotate the log file at 5-MB.

   log_filesize=5M.

c. Restart IIS Server

Deploying Public website pages using ConfigIIS.bat tool

About ConfigIIS.bat tool

From IC 7.3.3 onwards you can configure the following using the IIS configure tool:

- CSPortal Client
- CSPortal Server
- Public Website

The ConfigIIS.bat file is located at `<IC Install Path>\IC733WinIIS\bin` folder.

This script installs the Tomcat ISAPI filter, and map it to the virtual application /aicjakarta within the website provided.

The log files of the script are stored at the following location:

`<IC Install Path>\IC733WinIIS\IC733WinIIS\bin\ConfigIIS.log`.

The command format is:

`ConfigIIS.bat <Website Name> [options]`

Here:

- Website Name is the name of the website where the application is to be deployed.

  Note:
  When providing arguments with spaces in them, for example, Default Web Site, enclose them within quotes so that they are treated as a single argument such as, "Default Web Site".

- Options are:
  - CSPC to install CSPortal Client
  - CSPS to configure CSPortal Server information
  - WS to install Public Website pages

  Note:
  The options are case insensitive. Multiple options can be specified with a space as a delimiter.

CSPC) Configure CSPortal Client: When you select CSPC) Configure CSPortal Client option, the config tool installs the CSPortal Client to the IIS website, installs Tomcat Redirector, and creates a virtual application for the CSPortal Client in IIS.

CSPS) Configure CSPortal Server: When you select CSPS) Configure CSPortal Server option, the script installs the CSPortal Server to the IIS website. You must provide Fully Qualified Domain Name of the CSPortal Server and port at which the CSPortal Server is listening. The default port is 9699. The script sets the properties in the workers.properties file located at `<IC Install Path>\IC733WinIIS\tomcat\conf\` folder.

WS) Configure Public Website: When you select WS) Configure Public Website option, the script installs the Public Websie on the IIS.

Note:

The CSPC) Configure CSPortal Client option and CSPS) Configure CSPortal Server option is not applicable for public website pages deployment.

Configuring the application on the IIS website

Prerequisite:

You must add a website on Internet Information Server.

To configure the application on the IIS website:

1. Login to the server where the IIS website is configured.
2. Open Command prompt as an Administrator.
3. Go to `<IC Install Path>\IC733WinIIS\bin` folder.
4. Type **ConfigIIS.bat <Website Name>** and press **Enter**.

   The system displays the command line window with the following options:

   - CSPC) Configure CSPortal Client
   - CSPS) Configure CSPortal Server
   - WS) Configure Public Website
5. Type **WS** and press Enter to select WS)Configure Public Website.
6. Follow on-screen instructions.

Configuring Avaya Full Text Search Engine

Avaya Full Text Search Engine (Avaya FTSE) is the full text search engine for IC. Avaya FTSE supports the Web Self-Service database, including the FAQs and Suggested Email Responses.

This section includes the following topics:

- Configuring Avaya FTSE for Windows on page 248
- Configuring for Avaya FTSE for Oracle Solaris on page 250
- Configuring for Avaya FTSE for IBM AIX on page 253

Configuring Avaya FTSE for Windows

This section includes the following topics:

- Configuring full text searches for Microsoft Windows on page 248
- Updating the full text indices on Microsoft Windows on page 249

Configuring full text searches for Microsoft Windows

You must configure full text searches on every system that hosts one or more of the following:

- Customer website
- Administrative website
- WebACD server

To configure full text searches for Microsoft Windows:

1. Restart the IC website service, as described in Starting and stopping services on Windows on page 114.
2. Open a DOS command prompt window.
3. In the command prompt window, navigate to the following directory: *IC_INSTALL_DIR*\IC73\etc\wru_sql\

4. Run the set up command for your database as shown in the following table:

Database	Set up command
SQL Server	fulcrum_setup.cmd sqlserver <*ccq_database_username*> <*ccq_database_password*>
Oracle	fulcrum_setup.cmd oracle <*ccq_database_username*> <*ccq_database_password*>

   After the set up command executes, continue with Step 5.

5. Check the *IC_INSTALL_DIR*\IC73\etc\wru_sql\wru_createview.err file for errors.

   If the file is not present or is empty, then the set up command executed correctly. Some messages that you might see in the error file do not indicate a problem. For more information, see Full text search configuration error messages in the *Troubleshooting Interaction Center Guide*. Correct these errors as indicated in the message and as required by the database, then re-run the set up command

6. Check the *IC_INSTALL_DIR*\IC73\etc\wru_sql\fulcrum.err file for errors.

Updating the full text indices on Microsoft Windows

If you host your customer website and WebACD server on different systems, or if your IC configuration includes multiple websites, you must update the full text indices on those systems. The update ensures that the indices on these systems include all documents that you have added to the index.

You can run the update command as needed or schedule them to run at regular intervals. If you schedule an update to run at regular intervals, do not run the update more frequently than once per hour.

You must run this update command on every system that hosts one or more of the following:

- Customer-facing website
- WebACD server

Important:
Do not run this update command on the system that hosts the Administrative Website. That system automatically updates its own index.

To update the full text indices:

1. Open a DOS command prompt window.
2. In the command prompt window, navigate to the following directory: *IC_INSTALL_DIR*\IC73\etc\wru_sql
3. Run the following update command: **fulcrum_updatendx.cmd**

4. Check the *IC_INSTALL_DIR*\IC73\etc\wru_sql\fulcrum_updatendx.err file for errors.

   If the file is empty, then the set up command executed correctly. All messages in this file indicate errors. Correct these errors as indicated in the message and as required by the database, then re-run the set up command.

5. Restart the IC Website service, as described in Starting and stopping services on Windows on page 114.

   After you update the full text indices, you must restart the IC Website service to ensure that the drivers for the fulcrum search are loaded.

Configuring for Avaya FTSE for Oracle Solaris

This section includes the following topics:

- Changing ownership for the full text search directory on page 250
- Configuring full text searches on Solaris on page 250
- Updating full text indices on Oracle Solaris on page 253

Changing ownership for the full text search directory

Only the root user has read permissions for some of the files in the following directory: *IC_INSTALL_DIR*/IC73/etc/wru_sql

You must change the ownership for this directory if you plan to run the Avaya FTSE components as a non-root user on any system that hosts a Website or the WebACD server.

To change ownership for the full text search directory:

1. Log in as root user.
2. Navigate to *IC_INSTALL_DIR*/IC73/etc
3. Execute the following command:

   chown -R <*userid*> wru_sql

   where <*userid*> represents the non-root user that you use to run the Avaya FTSE components.

Configuring full text searches on Solaris

You must configure full text searches on every system that hosts one or more of the following:

- Customer Website.
- Administrative Website.

- WebACD Server.

To configure full text searches on Solaris:

1. If you defined the following environment variable in your shell, remove the setting for that environment variable.

Operating system	Environment variable
Solaris	ORACLE_HOME

2. Navigate to the following directory: *IC_INSTALL_DIR*/IC73/etc/wru_sql.
3. Run the following command to create the indices for full text searching:

   ./fulcrum_setup.sh <*ccq_database_username*> <*ccq_database_password*>

   When this command executes, you may see the following output:

Error message	Description
ERROR at line 1: ORA-00955: name is already used by an existing object	You can ignore this error. It indicates that the view already exists.
DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0601N The name of the object to be created is identical to the existing name "CCQ.WRU_VIEW" of type "VIEW". SQLSTATE=42710	You can ignore this error. This message indicates that the view already exists.

Error message	Description
"Error : 666"	This error indicates a problem in the odbc.ini file. This error results from the `bind18` command used to create bind packages for the ODBC drivers. Verify that the entries in the odbc.ini file for the `ccq` datasource are correct. Incorrect values in this file typically result from incorrect values entered in the Configuration Tool. Repeat the configuration of Web Self-Service.
execsql: execute failed SQLSTATE: SGS00, Native error: 0, error text [Hummingbird][SearchServer] Invalid table name	You may see this error message twice in fulcrum.err. This error occurs because the script is attempting to drop a table that does not yet exist. You can ignore this error when you run the `fulcrum_setup` command for the first time on a system. However, if you receive this error when you repeat the command on a system, investigate why the script cannot access the database to perform the following tasks: • unprotect table qw_wru_en • drop table qw_wru_en

4. Check the *IC_INSTALL_DIR*`/IC73/etc/wru_sql/fulcrum.err` file for errors.

   If the file is not present or is empty, then the set up command is executed correctly. Some messages that you might see in the error file do not indicate a problem. For more information, see Full text search configuration error messages in the *Troubleshooting Interaction Center Guide*.

5. Verify that the command did not create a file with a **`DIL`** extension in the *IC_INSTALL_DIR*`/IC73/etc/wru_sql/` directory.

   If such a file exists, check the contents for errors. If it contains errors, check the contents of `fulcrum_odbctrace.out` to see what went wrong. If there were problems with the database connection, confirm that the entries in the `odbc.ini` file are correct and that you invoked `fulcrum_setup.sh` with a valid username and password.

6. After you correct all errors, re-run the `fulcrum_setup.sh` command.

Updating full text indices on Oracle Solaris

If you host your customer website and WebACD server on different systems, or if your IC configuration includes multiple websites, you must update the full text indices on those systems. The update ensures that the indices on these systems include all documents that you have added to the index.

You can run the update command or schedule them to run at regular intervals. If you schedule an update to run at regular intervals, do not run the update more frequently than once per hour.

You must run this update command on every system that hosts one or more of the following:

- Customer-facing website.
- WebACD server.

Important:
Do not run this update command on the system that hosts the Administrative Website. The system that hosts the Administrative Website system automatically updates its own index.

To update the full text indices:

1. Navigate to the following directory: *IC_INSTALL_DIR*/IC73/etc/wru_sql
2. Run the following update command:

   ./fulcrum_updatendx.sh

3. Check the *IC_INSTALL_DIR*/IC73/etc/wru_sql/fulcrum_updatendx.err file for errors.

   If the file is empty, the set up command executed correctly. All messages in this file indicate errors. Correct these errors as indicated in the message and as required by the database, then re-run the set up command.

4. Restart the IC Website service, as described in Starting and stopping services on Solaris on page 115.

   After you update the full text indices, you must restart the IC Website service to ensure that the drivers for the fulcrum search are loaded.

Configuring for Avaya FTSE for IBM AIX

This section includes the following topics:

- Changing ownership for the full text search directory on page 254
- Configuring full text searches on IBM AIX on page 254
- Updating full text indices on IBM AIX on page 256

Changing ownership for the full text search directory

Only the root user has read permissions for some of the files in the following directory: *IC_INSTALL_DIR*/IC73/etc/wru_sql

You must change the ownership for this directory if you plan to run the Avaya FTSE components as a non-root user on any system that hosts a website or the WebACD server.

To change ownership for the full text search directory:

1. Log in as root user.
2. Navigate to *IC_INSTALL_DIR*/IC73/etc
3. Execute the following command:

   chown -R <*userid*> wru_sql

   where <*userid*> represents the non-root user that you use to run the Avaya FTSE components.

Configuring full text searches on IBM AIX

You must configure full text searches on every system that hosts one or more of the following:

- Customer Website
- Administrative Website
- WebACD Server

To configure full text searches on IBM AIX:

1. If you defined the following environment variable in your shell, remove the setting for that environment variable.

Operating system	Environment variable
IBM AIX	DB2DIR

2. Navigate to the following directory: *IC_INSTALL_DIR*/IC73/etc/wru_sql.

3. Run the following command to create the indices for full text searching:

   `./fulcrum_setup.sh <ccq_database_username> <ccq_database_password>`

   When this command executes, you may see the following output:

Error message	Description
ERROR at line 1: ORA-00955: name is already used by an existing object	You can ignore this error. It indicates that the view already exists.
DB21034E The command was processed as an SQL statement because it was not a valid Command Line Processor command. During SQL processing it returned: SQL0601N The name of the object to be created is identical to the existing name "CCQ.WRU_VIEW" of type "VIEW". SQLSTATE=42710	You can ignore this error. This message indicates that the view already exists.
"Error : 666"	This error indicates a problem in the odbc.ini file. This error results from the `bind18` command used to create bind packages for the ODBC drivers. Verify that the entries in the odbc.ini file for the `ccq` datasource are correct. Incorrect values in this file typically result from incorrect values entered in the Configuration Tool. Repeat the configuration of Web Self-Service.
execsql: execute failed SQLSTATE: SGS00, Native error: 0, error text [Hummingbird][SearchServer] Invalid table name	You may see this error message twice in fulcrum.err. This error occurs because the script is attempting to drop a table that does not yet exist. You can ignore this error when you run the `fulcrum_setup` command for the first time on a system. However, if you receive this error when you repeat the command on a system, determine the reason the script cannot access the database to perform the following tasks: • unprotect table qw_wru_en • drop table qw_wru_en

4. Check the *IC_INSTALL_DIR*/IC73/etc/wru_sql/fulcrum.err file for errors.

   If the file is not present or is empty, then the set up command is executed correctly. Some messages that you might see in the error file do not indicate a problem. For more information, see Full text search configuration error messages in the *Troubleshooting Interaction Center Guide*.

5. Verify that the command did not create a file with a **DIL** extension in the *IC_INSTALL_DIR*/IC73/etc/wru_sql/ directory.

   If such a file exists, check the contents for errors. If it contains errors, check the contents of fulcrum_odbctrace.out to see the issues. If there were problems with the database connection, confirm that the entries in the odbc.ini file are correct and that you invoked fulcrum_setup.sh with a valid username and password.

6. Verify that the wru_createview.sql script contains the correct values for username, password, and database name for the DB2 database.

   The Configuration Tool substitutes these values when you configure the Website Web application. Incorrect values in this file typically result from incorrect values entered in the Configuration Tool. If the file includes errors, re-configure the Website. For more information, see Configuring Web Management services on page 206.

7. If necessary, after you correct all errors, re-run the fulcrum_setup.sh command.

Updating full text indices on IBM AIX

If you host your customer website and WebACD server on different systems, or if your IC configuration includes multiple Websites, you must update the full text indices on those systems. The update ensures that the indices on these systems include all documents that you have added to the index.

You can run the update command as needed or schedule them to run at regular intervals. If you schedule an update to run at regular intervals, do not run the update more frequently than once per hour.

You must run this update command on every system that hosts one or more of the following:

- Customer-facing Website
- WebACD Server

Important:
Do not run this update command on the system that hosts the Administrative Website. That system automatically updates its own index.

To update the full text indices:

1. Navigate to the following directory: *IC_INSTALL_DIR*/IC73/etc/wru_sql
2. Run the following update command:

   ./fulcrum_updatendx.sh

3. Check the *IC_INSTALL_DIR*/IC73/etc/wru_sql/fulcrum_updatendx.err file for errors.

   If the file is empty, the set up command executed correctly. All messages in this file indicate errors. Correct these errors as indicated in the message and as required by the database, then re-run the set up command.

4. Verify that:
   - The odbc.ini file lists the IP address of the DB2 system not the hostname.
   - Each IP address listed in /etc/hosts has only one entry.

5. Restart the IC Website service, as described in Starting and stopping services on AIX on page 118.

   After you update the full text indices, you must restart the IC Website service to ensure that the drivers for the fulcrum search are loaded.

Configuring Web Scheduled Callback

Web Scheduled Callback uses the components of the IC chat channel to route and report on website customer requests for an agent callback.

Tip:
If you want an agent to handle Web Scheduled Callback contacts, you must configure the agent to handle voice and chat contacts.

To configure Web Scheduled Callback:

1. Cautions and tips for configuring Web Scheduled Callback on page 257
2. Creating a Web Scheduled Callback server on page 258
3. Configuring the Website for Web Scheduled Callback on page 259
4. Configuring Agents for Web Schedule Callback on page 260

Cautions and tips for configuring Web Scheduled Callback

This section includes some important cautions and tips that you need to consider when you install the software for Avaya Agent Web Client on the server.

This section includes the following topics:

- Supported agent desktop applications on page 258
- Time zone requirements for Web Scheduled Callback on page 258

- Calendar requirements for Web Scheduled Callback on page 258

Supported agent desktop applications

Avaya Agent, Avaya Agent Web Client and custom application, developed with the Client SDK, support Web Scheduled Callback.

Time zone requirements for Web Scheduled Callback

Web Scheduled Callback is a time-bound feature. For Web Scheduled Callback to work correctly, all IC servers and the database must be in the same time zone.

Important:
If the time on the systems that host IC servers and the database is not synchronized, a time lag may occur between the scheduled time for the callback and the exact time that a Web Scheduled Callback request is delivered to an agent.

Calendar requirements for Web Scheduled Callback

Web Scheduled Callback requires the Gregorian calendar. Web Scheduled Callback does not work with any other calendar. For example, Web Scheduled Callback does not support the Thai B. E. (Buddhist Era) calendar or date format.

Creating a Web Scheduled Callback server

The Web Scheduled Callback server retrieves the scheduled call from the database and delivers the call to the agent as a Chat&Callback task.

To create a Web Scheduled Callback server:

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **WSCallback** and click **Ok**.
3. On the **General** tab enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	WSCallback_<*domain*>	Include the domain in the server name to identify the server.

Field	Recommended entry	Notes
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Website` from the drop-down list.
Host	Enter or select the IP address from the drop-down list.	When you select the host, IC Manager fills in the corresponding Directory, Port, and Executable.

4. Click the **WSCallback** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
ICM Server Name	Enter the name of the system where the ICM server is installed.	The Web Scheduled Callback contacts are sent to the ICM server that you specify here.
Call timeout interval (sec)	Enter the number of seconds after which the time out occurs if the request is not routed to an agent.	Default is 120.
IC Login	Enter the IC Login username.	Default is dcobridge1
IC Password	Click the Ellipsis (…) and specify the password for the IC Login.	

5. Click **Ok**.

Configuring the Website for Web Scheduled Callback

You can configure the working hours of a contact center with the tenant properties for a Website. The default values for these properties assume that the contact center opens at 09:00 and closes 18:00.

To configure the Website for Web Scheduled Callback:

1. In IC Manager, select **Services** > **MultiTenancy Administration**.
2. In the **Tenant Admin** menu, select **Tenant Properties**.
3. From the **Select a Tenant** drop-down list select the tenant you want to customize.
4. Click **Customize Tenant**.
5. On the **Customize Tenant** page, select the language properties you want to set from the **Select Language** drop-down list at the top of the page.
6. Click the **Callback** link.

7. Update the properties mentioned in the following table, and then click **Update Data**.

Property	Default value	Notes
callback.checkcallbacktime	TRUE	When set to TRUE, enables Web Scheduled Callback.
callback.contactcenteropentime	09:00	Use a 24-hour clock and xx:xx format only.
callback.contactcenterclosetime	18:00	Use a 24-hour clock and xx:xx format only.

Configuring Agents for Web Schedule Callback

Agents can receive the Web Schedule Callback only if the chat and voice channels are enabled for them.

To configure the agents for Web Schedule Callback:

1. Create a new Workgroup:
   a. In IC Manager, select **Tools** > **Groups**.
   b. The **Group Manager** window opens.
   c. In the left pane, right-click the **DefaultTenant** and select **New Workgroup**.
   d. In the **Create New Workgroup** window, enter the value for **Workgroup Name** and the **Description**.
   e. Click **Ok**.
   f. Add all the agents who are handling the Web Schedule Callback requests to this workgroup.
   g. Click **Ok**.
2. Create a new Queue:
   a. In IC Manager, click the **Device** tab.
   b. In the left pane, right-click **Devices** and select **New Device**.
   c. In the list of devices, select **Chat Queue**.

d. In **Device Editor**, enter the value for the fields mentioned in the following table:

Field	Value
QueueID	Enter the queue ID for the queue. For example, `ScheduledCallbackQueue`.
Name	Enter the name for the queue. You can enter the queue ID as queue name.
Priority	Enter the queue priority value as 1.
Minimum Agents	Enter the minimum number of agents as 1.
Workgroup	Enter the queue membership. Click the **Ellipses (...)** button next to the field and add the workgroup that you have created in the first step to be a member of this queue.
Tenant	The value for this field is automatically selected based on the workgroup that you select.

e. Click **Ok**.

In the right pane, the queue is added in the list of devices.

3. Create Routing Hints:

a. In IC Manager, click the **Configuration** tab.

b. In the left pane, select **Tables** > **WorkFlow** > **RoutingHint**.

c. On the toolbar, click the **New** button.

d. Add the following two routing hints:

Note:

Add routing hints for all the languages that your call center supports by using the standard language conventions as Routing Hint names.

Routing Hint	Chat Queue ID	Tenant
en	Enter the chat queue ID that you have created in the step 2. For example, `ScheduledCallbackQueue@DefaultTenant`.	Select the Tenant for the queue ID that you select.
pvchat	Enter the chat queue ID that you have created in the step 2. For example, `ScheduledCallbackQueue@DefaultTenant`.	Select the Tenant for the queue ID that you select.

4. Build and upload the routing hints to the workflow.
   a. In IC Manager, click the **Servers** tab.
   b. In the right pane, select the **WorkFlow** server from the list of servers.
   c. Click the **WorkFlow** tab.
   d. Click the **Run Flow** button.
   e. Keep the default value for flow name.
   f. Click **Ok**.
   g. Click **Ok**.

Configuring Voice Chat

Avaya Interaction Center (Avaya IC) installations can include Voice Chat. Voice Chat is a component of Web Management that includes the following features:

- Chat and VoIP where a voice chat contact is initiated from a chat session. The customer uses VoIP, and the agent uses a telephone.
- Chat and Phone where a voice chat contact is initiated from a chat session. The customer and the agent use a telephone.

VoIP Chat feature is incorporated in the HTML Chat client. This feature enables customer and agent to communicate using a VoIP call during an HTML chat session.

To set up both types of VoIP Chat, perform the steps in the following topics:

1. Prerequisites for Voice Chat on page 263
2. Configure the Workflow server for Voice Chat on page 267
3. Build and load workflows for Voice Chat on page 270
4. Configure the Telephony server for Voice Chat on page 271
5. Configure the Voice Chat gateway on page 272
6. Configure the Voice Media Manager server on page 273
7. Configure the Voice Chat workflow table on page 274
8. Set the startup options for the VMM server on page 275
9. Configuring IC System for Voice Chat on page 276

Prerequisites for Voice Chat

Before you configure Voice Chat:

1. Install and configure the Telephony switch and other hardware, including the following:
   - Install and configure a supported IP Gateway
   - Create a separate route point (VDN) for Voice Chat
   - Direct all calls on the Voice Chat route point (VDN) over the CTI link using the Adjunct Route

   For information about supported Telephony switches, see VoIP Configuration on page 263. For information about your Telephony switch, see the switch documentation.
2. Install and configure Telephony, including an ACD. For more information, see *Avaya IC Installation and Configuration* guide.
3. Install and configure Web Management. For more information, see *Avaya IC Installation and Configuration* guide.
4. Confirm that the Avaya Voice Media Manager (VMM) is installed and running. The Voice Media Manager does not run in IC Manager. On a Windows system, you can view and start the Voice Media Manager in the Services Control Panel.

   Avaya IC installs the VMM with the Avaya IC servers.

VoIP Configuration

This section explains how to configure the Avaya DEFINITY/Communication Manager switch to enable the Voice channel to handle VoIP calls. This section contains the following configurations:

- Define IP Codec Set on page 264
- Assign node name on page 264
- Define the IP interface on page 264
- Assign a link to the C-LAN on page 265
- Create an IP signaling group on page 265
- Create IP trunk group on page 266
- Define the class of restriction on page 266
- Create vector for route point (VDN) on page 267

Define IP Codec Set

To define the Codec Set:

1. Run **change ip-codec-set 1** on the command line.

   The **change ip codec set 1** form opens.
2. Type **G.723-5.3K** in the **Audio Codec** field.
3. Type **Y** in the Silence **Suppression** field.
4. Type **1** in the **Frames Per Pkt** field.
5. Type **30** in the **Packet Size (ms)** field.
6. Press **F3** to submit this form.

Assign node name

You need to add a node name for the C-LAN, TN2302 Medpro board and VMM server.

To assign the node name

1. Run **change node-names ip** on the command line.

   The **node names ip** form opens.
2. Type the unique name for each C-LAN and for each TN2302 Medpro board in the **Name** field.

   Note:

   If you use CrossFire board TN2602, you may get an error message as **IP Codec mismatched**. The Communication Manager must have at least one TN2302 Medpro board to work with Voice chat, as the VMM service requires the G.723-5.3 IP codec.
3. Type the unique IP address for each of the corresponding C-LAN and TN2302 Medpro board in the **IP Address** field.
4. For the VMM Server, type the hostname in the **Name** field and IP address in the **IP Address** field.
5. Press **F3** to submit this form.

Define the IP interface

To define the IP interface for CLAN

1. Run **change ip-interface <board location>** on the command line.

   The **IP interface** form opens.
2. Type **y** in the **Enable Ethernet Port** field.

3. Type the node name that you created for the C-LAN circuit pack in Assign node name on page 264 in the **Node Name** field.
4. Type the IP address of the gateway for the ip interface for the C-LAN circuit pack in the **Gateway Address** field.
5. Type `1` in the **Network Region** field for the C-LAN circuit pack.
6. Press **F3** to submit this form.

To define the IP interface for Medpro

1. Run `change ip-interface <board location>` on the command line.

   The **IP interface** form opens.
2. Type `y` in the **Enable Ethernet Port** field.
3. Type the node name that you created for the TN2302 Medpro board in Assign node name on page 264 in the **Node Name** field.
4. Type the IP address of the gateway for the ip interface for the TN2302 Medpro board in the **Gateway Address** field.
5. Type `1` in the **Network Region** field for the TN2302 Medpro board.
6. Press **F3** to submit this form.

Assign a link to the C-LAN

You must assign a link to the C-LAN using the ethernet data module.

To assign a link to the LAN using the ethernet data module

1. Run `add data-module next` on the command line to open the **data module** form.
2. Type `Ethernet` in the **Type** field.
3. Type the port number to be used by the C-LAN circuit pack in the **Port** field. Ethernet connections must be assigned to port 17 on the C-LAN circuit pack.
4. Type the link number to assign to the circuit pack in the **Link** field.
5. Press **F3** to submit this form.

Create an IP signaling group

To create a signaling group:

1. Run `add signaling-group next` on the command line to open the **signaling group** form for the next available signaling group.
2. Type `h.323` in the **Group Type** field.

3. Leave the **Trunk Group for Channel Selection** field blank until you create a trunk group in the next task. After you have created the trunk group, run **`change signaling group`** at the command line and enter the trunk group number in the **Trunk Group for Channel Selection** field.
4. Type the node name that you created for the C-LAN IP interface in Assign node name on page 264 in the **Near-end Node Name** field.
5. Type the port number **`1720`** for the C-LAN IP interface in the **Near-end Listen Port** field.
6. Enter the node name of the VMM server you created in Assign node name on page 264 in the **Far-end node name** field and the port created in IC Manager for VMM (default 8120) in **Far-end Listen Port** field.
7. Press **F3** to submit this form.

Create IP trunk group

To create a trunk group:

1. Run **`add trunk-group next`** on the command line.

   The **trunk group** form opens.
2. Type **`isdn`** in the **Group Type** field.
3. Type **`IP Trunk`** in the **Group Name** field.
4. Type the trunk access code in the **TAC** field.
5. Type **`H.323`** in the **Carrier Medium** field.
6. Type **`tie`** in the **Service Type** field.
7. Type **`auto`** in the **Member Assignment Method** field.
8. Enter the number of the signaling group from the previous task, Create an IP signaling group on page 265 in the **Signaling Group** field.
9. Enter number of members in the **Number of Members** field for this trunk.
10. Press **F3** to submit this form.

Define the class of restriction

To define the class of restriction 1:

1. Run **`change cor 1`** at the command line to open the **cor 1** form which is used by all trunk groups.
2. Enter **`0`** (zero) in the **FRL** field.
3. Enter **`none`** in the **Calling Party Restriction** field.
4. Enter **`none`** in the **Called Party Restriction** field.
5. Press **F3** to submit this form.

Create vector for route point (VDN)

To create vector for route point:

1. Run **`change vector <vector number>`** at the command line to open the **CALL VECTOR** form.

   The vector number is the number that you have mentioned in the VDN.

2. Create a vector layout as follows:

```
wait-time 2 secs hearing ringback
adjunct routing link 5
wait-time 5 secs hearing ringback
stop
```

3. Press **F3** to submit this form.

Configure the Workflow server for Voice Chat

To configure the Workflow server for Voice Chat, perform the steps in the following topics:

1. Add a semaphore for the Voice Chat workflow on page 267
2. Create the Voice Chat channel for the Workflow server on page 268
3. Restart the Workflow server on page 269

Note:

This section assumes that you are using an existing Workflow server to handle Voice Chat contacts. If the Avaya IC system includes a separate Workflow server for Voice Chat, see *IC Avaya IC Installation and Configuration* guide.

Add a semaphore for the Voice Chat workflow

You must add a semaphore to all Workflow servers that process voice chat contacts and are in the Web and Website domain. The Attribute server uses the ICM account to log in to the ICM server. You entered this account in the **IC Login** field of the Attribute server configuration. For more information about the icmbridge account, see *Avaya IC Installation and Configuration*.

To add the semaphore for the Voice Chat workflow:

1. In IC Manager, double-click the Workflow server.
2. Click the **Workflow** tab.
3. Click the **Ellipsis (...)** button next to **Semaphores**.
4. In the **Semaphores** dialog box:
   a. Click **New**.

b. Click in the new row and type:

```
ivchat.ivchat_key
```

c. Click **OK**.

5. Click **OK**.

Create the Voice Chat channel for the Workflow server

If your Avaya IC system includes multiple Workflow servers, perform the following steps on the Workflow server that processes voice contacts.

To create the voice chat channel for the Workflow server:

1. In IC Manager, double-click the Workflow server that processes voice contacts.
2. Click the **Channels** tab.
3. Select **New Channel**.
4. In the **Channel Editor** dialog box, complete the fields as shown in the following table and select **OK**.

Field	Recommended entry	Notes
Global	Do not select this field.	Do not select this field to create a channel for a specific server or media, such as Voice Chat.
By Server	• Do not select this field if you want this channel to handle events from all servers of the type that you select from the **Service** drop-down list. • Select this field if you want this channel to handle events from only one specific server that you select from the **Service** drop-down list.	If you select this field, and you need this Workflow server to communicate with more than one server, you must create another channel for that server. **Warning:** If you select this field and the Telephony server is named "TS", the Workflow server cannot communicate with the Telephony server.
Channel Range	No entry necessary.	Completed by IC Manager.

Field	Recommended entry	Notes
Service	Select **TS** or a specific Telephony server from the drop-down list.	Whether you can select a server or a type of server, depends up whether or not you selected the **By Server** field.
Criteria	Type: ***r<VDN_for_Voice_Chat>**	The VDN that you have created as mentioned in the Prerequisites for Voice Chat on page 263. For example, type: ***r57001**

5. Select the channel that you created in the step above.
6. Select **New Association**.
7. In the **Channel Association** dialog box, complete the fields as shown in the following table and select **OK**.

Field	Recommended entry
Channel Range	Completed by IC Manager.
Service Interface	Completed by IC Manager.
Event	TS.IncomingCall **Note:** This field is case-sensitive.
Flow	***<project_name>.<flow_name>*** For example, type ts.incoming_ivchat

Restart the Workflow server

To restart the Workflow server:

1. In IC Manager, select the Workflow server that handles voice contacts.
2. Right-click the **Workflow server** and select **Stop**.
3. After the Alarm Monitor at the bottom of IC Manager displays a message confirming that the Workflow server has stopped:
   a. Select the **Workflow server**.
   b. Right-click the **Workflow server**.
   c. Select **Start**.

Build and load workflows for Voice Chat

Voice Chat uses the following sample workflows:

- Incoming Voice Chat workflow in the TS project.
- Voice Chat workflow in the ivchat project.
- Telephony workflows, see *Avaya IC Installation and Configuration.*

The Avaya IC seed data does not include a compiled sample Voice Chat or a compiled sample Incoming Voice Chat workflow. You must build and load these workflows.

CAUTION:
By default, the Qualify Chat workflow assumes that you will create a WebVoice workgroup that includes agents who are configured to receive contacts from the voice and chat channels. If you do not intend to create this workgroup, you must customize the `IVChatWorkgroup` and `PVChatWorkgroup` properties in the Set Route Parameter blocks. The value of these properties must be the name of a valid workgroup. The workgroup must include agents who can handle contacts from the voice and chat channels. If you change these blocks, you must build and load the Qualify Chat workflow.

For more information about voice chat workflows and Workflow Designer, see Avaya Workflow Designer User Guide.

To load the Voice Chat workflows, complete the steps in the following topics:

1. Build the Incoming Voice Chat workflow on page 270
2. Build the Voice Chat workflow on page 271

Build the Incoming Voice Chat workflow

To build the Incoming Voice Chat workflow:

1. In Workflow Designer, select **File** > **Open Project** and open the TS project.

   You can find the TS project in the following directory:

   IC_INSTALL_DIR`\IC73\design\IC\Flows\Avaya\TS\TS.prj`
2. Double-click **incomingivchat.qfd** in the **Project** pane.
3. Select **Project** > **Settings**.
4. Select the **Database** tab and type the following values:
   - Interaction Center Data Source name in the **IC Data Source** field.
   - Valid Avaya IC Administrator account in the **Login ID** field.

     The default account is Admin.

- Password for the account in the **Password** field.

5. Click **OK**.
6. Select **Build** > **Build Flowset**.

   Workflow Designer verifies and compiles the flows. All error messages, including the block name, script name, and offending line, are displayed in the Output bar.
7. Select **File** > **Exit** to exit Workflow Designer.

Build the Voice Chat workflow

To build the voice chat workflow:

1. In Workflow Designer, open the Voice Chat workflow located in the following directory:

   IC_INSTALL_DIR\IC73\design\IC\flows\Avaya\ivchat\ivchat.qfd
2. Select **Project** > **Settings**.
3. Select the **Database** tab and type the following values:
   - Interaction Center Data Source name in the **IC Data Source** field.
   - Valid Avaya IC Administrator account in the **Login ID** field.
   - Password for the account in the **Password** field.
4. Click **OK**.
5. Select **Build** > **Build Flowset**.

   Workflow Designer verifies and compiles the flows. All error messages, including the block name, script name, and offending line, are displayed in the Output bar.

Configure the Telephony server for Voice Chat

You must configure the Telephony server to ensure that the agent is not placed in a Busy state and can receive a voice chat contact.

To configure the Telephony server for Voice Chat:

1. In IC Manager, double-click the Telephony server.
2. Click the **TS** tab.
3. Right-click in the background and select the check box adjacent to **Show Advanced Properties**.
4. Select the **Dial By Equipment** check box.

   You might need to scroll down to see the **Dial By Equipment** check box.
5. Click **OK**.

Configure the Voice Chat gateway

You must configure one Voice Chat gateway for each CLAN card. Repeat the following steps for each gateway:

To configure the Voice Chat gateway:

1. In IC Manager, click the **Configuration** tab.
2. From the **Tables** list in left pane, select **Voice Chat** > **IPGateway**.
3. Click **New**.
4. In the right pane, enter the value for the fields mentioned in the following table:

Field	Recommended entry	Description
Name	Type a unique name for the gateway.	For example, type the node name of the CLAN card.
IP Address	Type the IP Address of the CLAN card.	
Port	Type the near end listening port of the CLAN card. Default: `1720`	
ACD Name	Select the name of the ACD from the drop-down list.	Select the same ACD that you configured for the Telephony server.
Site	Select the site from the drop-down list.	For example, select `DefaultSite`.
RoutePoint	Type the VDN that you set up in the switch to receive voice chat calls.	

Field	Recommended entry	Description
Capacity	Type the number of calls which this gateway can handle.	Check your switch documentation for more information.
Active	Select this check box if you want voice chat to be able to use the gateway.	Gateways should always be active unless there is a problem with the gateway, or you must perform maintenance on the system. If there is a problem with a gateway, clear this check box immediately to ensure the gateway cannot be used for subsequent calls. Before you bring the system that hosts the gateway down for maintenance, make the gateway inactive so that it is not used for the subsequent calls. You can bring the system down as soon as there are no more calls on the gateway.

5. Click **OK**.

Configure the Voice Media Manager server

Avaya IC installs the Voice Media Manager (VMM) server when you install Avaya IC servers on a system. You can configure and run more than one VMM server in an Avaya IC system.

Avaya IC uses a round robin algorithm to select a VMM server from an available list of VMMs to handle a voice chat.

To configure the VMM Server:

1. In IC Manager, click the **Configuration** tab.
2. From the Tables list in left pane, select **Voice Chat** > **VMM**.
3. Click **New**.

4. In the right pane, enter the value for the fields mentioned in the following table:

Field	Recommended entry	Description
Name	Type the name of the system that hosts the VMM server.	For example, if host the VMM server on testbox.xyzcorp.com, type "testbox" as the name of that VMM server.
IP Address	Type the IP Address of the system that hosts the VMM server.	
Port	Default 8120.	
Site	Select the site from the drop-down list.	For example, select `DefaultSite`.
Active	Select this check box.	A VMM server should always be active unless there is a problem with the VMM server, or you must perform maintenance on the system. If there is a problem with a VMM server, clear this check box immediately to ensure the VMM server cannot be used for subsequent calls. Before you bring the system that hosts the VMM server down for maintenance, make the VMM server inactive so that it is not used for the subsequent calls. You can bring the system down as soon as there are no more calls on the VMM server.

5. Click **OK**.

Configure the Voice Chat workflow table

To configure the Voice Chat workflow table:

1. In IC Manager, click the **Configuration** tab.
2. From the Tables list in left pane, select **Workflow** > **VoiceChat**.
3. Click **New**.

4. In the right pane, enter the value for the fields mentioned in the following table:

Parameter	Recommended entry	Description
Name	Type the name of the IV chat workflow.	For example, type ivchat.
Timeout (sec)	Type the number of seconds that the workflow should wait before it times out.	This entry represents how many seconds a gateway should have to respond to a **`MakeCall`** request.

5. Click **OK**.

Set the startup options for the VMM server

The VMM setup script configures the VMM to start automatically.

If you host your Avaya IC servers on Solaris, you must run the VMM setup script to start and configure the Voice Media Manager (VMM) for Voice Chat.

Important:
You must perform this step only if you host your Avaya IC servers on Solaris.

You must set the VMM server to autostart, as described in the following topics:

- Set the startup options for the VMM server on Windows on page 275
- Set the startup options for the VMM server on Solaris on page 275

Set the startup options for the VMM server on Windows

To set startup options for the VMM server on Windows:

1. In the Services control panel, right-click **Avaya Voice Media Manager** and select **Properties**.
2. Select **Automatic** from the **Startup Type** drop-down list.
3. Click **OK**.

Set the startup options for the VMM server on Solaris

To configure the VMM server to start automatically 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**.

To stop the VMM server on Solaris:

1. Navigate to the following directory:

   IC_INSTALL_DIR/IC73/bin

2. At the command line, type:

   ./vmm_setup stop

3. Press **Enter**.

Configuring IC System for Voice Chat

To enable the VoIP feature to function properly, you need to configure your IC system. Before performing the steps given below, you need to carry out all of the installation instructions described in Configuring Voice Chat on page 262.

Note:
VoIP Chat is only supported on Windows and Solaris.

Configuring Website for Voice Chat

1. Launch the Web browser and navigate to the Website Admin Pages.
2. Navigate to the **IC Website Multi-tenant Administration** page and select **Tenant Properties**.
3. Click **Customize**.
4. Select **Chat Properties**.
5. Modify the following chat properties:

   VoIP Chat requires the size of the command frame to be changed to **120** so that the VoIP applet can be placed in the command frame

   - Change the **chat.htmlclient.command.framesize** property value from the default size of **55** to **120**. This modification is required to fit the VoIP chat applet in the command frame.
   - Change the **chat.phrases.IccCommon.launchvoip** property value to **Agent has initiated Voice Chat.**

6. Click **Update Data** to save the changes.

Setting up a separate administration Website (optional)

You can configure a web server to serve as an administration website only. The administration website does not contain any accessible external or customer-facing content, and the chat functions are disabled.

These instructions assume that you have already configured Web Management.

Note:
If your IC system includes multiple Attribute servers, all Websites and ICM servers must use the same Attribute server, so that their Tenant customization properties remain synchronized.

To set up a separate administration website, complete the steps in the following topics:

1. Creating the Web application for the administration website on page 277
2. Configuring an administration Website on page 277
3. Integrating the administration Website on page 278

Creating the Web application for the administration website

Create the Web application for the administration website, as described in Configuring Web Management services on page 206.

Configuring an administration Website

Create a separate entry for the administration Website in IC Manager.

To configure the administration website:

1. In IC Manager, click the **Configuration** tab.
2. From the **Tables** list in left pane, select **Website** > **Website Context Configuration**.
3. Click **New**.
4. Right-click in the right pane, and select the box next to **Show Advanced Properties**.

5. Complete the fields in the right pane, as shown in the following table:

Field	Recommended entry
Global Name	Type a name for the website. For example, type AdminWebsite. **Note:** The Global Name is case-sensitive. The Global Name must match the **dsObject** parameter in the following file on the system that hosts the administration Website: *IC_INSTALL_DIR*\IC73\comp\website\WEB-INF\web.xml
Context Active	Select this box.
Admin Pages Active	Select this box.
Public Pages Active	Do not select this box.

   For more information about these fields, see Configuring the Website on page 241
6. Click **Ok**.
7. Select **Manager** > **Refresh**.
8. Restart the Tomcat server that hosts the Administration website.

Integrating the administration Website

To integrate the administration website:

1. In IC Manager, select **Tools** > **Groups**.
2. Select the **Properties** tab.
3. Select **IC** in the left pane of the **Group Manager**.
4. Select **System/Configuration** in the Sections list.
5. Select the following properties:
   a. Select **Edit**.

b. Set values for the properties, as shown in the following table:

Property	Recommended entry
ChatLoginServer	Type the fully-qualified domain name of the system that hosts the administration website.
ChatLoginServerWebsite	Type the servlet context name that you gave to this website in Configuring an administration Website on page 277.

Note:
If the columns in the right pane are Name, Entity, Value, and Overridable, select the **- (minus)** button on the toolbar to view and edit these properties.

6. Click **Ok**.

Setting up a separate customer Website (optional)

You can configure a web server to serve as a customer website only. The customer website does not contain any accessible administration functions. These instructions assume that you have already configured Web Management.

Note:
If the IC system includes multiple Attribute servers, all Websites and ICM servers must use the same Attribute server, so that their Tenant customization properties remain synchronized.

To set up a separate customer Website, complete the steps in the following topics:

1. Creating the Web application for the customer Website on page 279
2. Configuring the customer Website on page 279

Creating the Web application for the customer Website

Create the Web application for the customer website, as described in Configuring Web Management services on page 206.

Configuring the customer Website

Create a separate entry for the customer website in IC Manager.

To configure the customer website:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Website** > **Website Context Configuration**.
3. Select **New**.
4. Right-click in the right pane, and select the box next to **Show Advanced Properties**.
5. Complete the fields in the right pane, as shown in the following table:

Field	Recommended entry
Global Name	Type a name for the Website, for example, type CustomerWebsite.
Context Active	Select this box.
Admin Pages Active	Do not select this box.
Public Pages Active	Select this box.

   For more information about these fields, see Configuring the Website on page 241
6. Click **Ok**.
7. Select **Manager** > **Refresh**.
8. Restart the Tomcat server that hosts the customer website.

Deploying multiple ICM servers (optional)

The ICM server hosts the Web Management conferences between agents and customers. You can deploy additional ICM servers, for one or both of the following reasons:

- To increase the capacity or load sharing of chat functionality.
- To use a secure server for chat escalations from one site but not another.

Tip:
The procedures in this section describe how to deploy one additional ICM server. To deploy more than one additional ICM servers, follow these instructions for each additional ICM server.

This section includes the following topics:

- Deployment guidelines for an additional ICM server on page 281
- Before you configure an additional ICM server on page 281

- Configuring an additional ICM server with a CIRS server on page 282
- Configuring an independent additional ICM server on page 285
- Adding ICM servers to the ICM Bridge on page 286

Deployment guidelines for an additional ICM server

The following guidelines describe the two ways that you can deploy an ICM server:

Deploying an additional ICM server with a CIRS server: With a CIRS server for load balancing. In this configuration, users enter the website on the primary system and are redirected to an ICM server on a different system based on the load. For more information, see Configuring an additional ICM server with a CIRS server on page 282.

Deploying an additional ICM server without a CIRS server: Without a CIRS server. In this configuration, each combination of ICM server and website is independent. For more information, see Configuring an independent additional ICM server.

Tip:
If you are setting up a secure ICM server, follow the instructions in the section Configuring IC Websites over HTTPS on page 304, as well as the instructions in the following procedures.

Before you configure an additional ICM server

This section includes steps you must perform before you configure an additional ICM server.

This section includes the following topics:

- Location of an additional ICM server on page 281
- Installing the ICM server software on page 282
- Setting the startup options for the secondary ORB server on page 282

Location of an additional ICM server

Deploy an additional ICM server, on a dedicated system, for scalability. Do not install the additional ICM server on the system that hosts your database software.

Installing and configure prerequisites

Install and configure all prerequisites for a website system, including a database client. For more information, see *Avaya IC Installation Planning and Prerequisites*.

Installing the ICM server software

The software for the ICM server is included in the IC installer for IC servers. To install the ICM server software, follow the instructions in Installing IC server components on page 35.

Setting the startup options for the secondary ORB server

If you do not plan to host other IC servers on the same system as the additional ICM server, then do not start the secondary ORB server. Set the startup options on the secondary ORB server to **Manual**.

If the system also hosts an IC server, such as an Attribute server, the secondary ORB server must be started. Set the startup options for the secondary ORB server to **Automatic**.

For more information on how to set the startup options, see Starting and stopping the ORB server on page 110.

Configuring an additional ICM server with a CIRS server

To configure an additional ICM server to work with a CIRS server and the website, you must designate one system that hosts an ICM server and website combination as the primary ICM server system.

Note:
You must create a website on the secondary system, where you are configuring another ICM server with the CIRS server.

After you determine which system is the primary ICM server system, perform the steps in the following topics:

1. Configuring the primary ICM server on page 282
2. Configuring the additional ICM server on page 283
3. Configuring the CIRS server on page 284
4. Configuring the CIRS servlet for Website on page 285
5. Adding ICM servers to the ICM Bridge on page 286

Configuring the primary ICM server

These instructions assume that you have already installed and configured the primary ICM server and the CIRS server.

To configure the primary ICM server:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Chat** > **ICM**.

3. Select the ICM table with the same name as the **dsObjectName** in *IC_INSTALL_DIR*/IC73/etc/SystemParms.txt

   If the table does not exist, create a new table. For more information, see Configuring the ICM server on page 237.

4. Update the fields in the right pane shown in the following table:

Property	Recommended entry
Global ICM Name	Type the value of **dsObjectName**.
ICM Server Name	Type the fully-qualified domain name of the system that hosts the primary ICM server.
CIRS Host	Type the hostname of the system that hosts the primary ICM server.
CIRS Port	Type the port for the CIRS server.

   For information on all other fields, see Configuring the ICM server on page 237.

5. Click **Ok**.
6. Restart the ICM server.
7. Start the CIRS server.
8. Add the ICM server to the ICM Bridge. For more information, see Adding ICM servers to the ICM Bridge on page 286.

Configuring the additional ICM server

To configure the additional ICM Server:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Chat** > **ICM**.
3. Select **New**.

4. Update the following fields in the right pane shown in the following table:

Property	Recommended entry
Global ICM Name	Type a name for the additional ICM server. For example, type **icm2**.
ICM Server Name	Type the fully-qualified domain name of the system that hosts the additional ICM server.
CIRS Host	Type the hostname of the system that hosts the primary ICM server.
CIRS Port	Type the port for the CIRS server.

   For information on all other fields, see Configuring the ICM server on page 237.

5. Click **Ok**.
6. Restart the ICM server.
7. Start the CIRS server.
8. Add the ICM server to the ICM Bridge. For more information, see Adding ICM servers to the ICM Bridge on page 286.

Configuring the CIRS server

To configure the CIRS server:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Chat** > **CIRS**.
3. Select the CIRS table with the same name as the **dsObjectName** in *IC_INSTALL_DIR*/IC73/etc/cirsParms.txt

   If the table does not exist, create a new table. For more information, see Configuring the Central Internet Routing service on page 240.

4. In the **Global CIRS Name** field in the right pane, type the value of **dsObjectName** in *IC_INSTALL_DIR*/IC73/etc/cirsParms.txt

   For information on all other fields, see Configuring the Central Internet Routing service on page 240.

5. Select the **CIRS Active** check box.

   This check box must be selected for the CIRS server to function.

6. Click **OK**.
7. Start the CIRS server.

Configuring the CIRS servlet for Website

For more information about Website applications, see Configuring the Website on page 241.

To configure the CIRS servlet for website:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Website** > **Website Context Configuration**.
3. Create or update the websitecontext record for each Web Management application that chat users must access.
   a. On the toolbar, click to create a new record.
   b. Right-click and select the **Show Advanced Properties** check box.
   c. Complete the fields as shown in the following table:

Property	Recommended entry
Global Name	Type the value of `dsObjectName` in *`IC_INSTALL_DIR`*`/IC73/comp/website/WEB-INF/web.xml`.

   For information on all other fields, see Configuring the Central Internet Routing service on page 240.
4. Click **Ok**.
5. Restart each server that hosts a website application.
6. Start the ICM server.

Configuring an independent additional ICM server

After you designate one system as the primary ICM server system, perform the steps in the following topics:

1. Configuring an additional ICM server on page 285.
2. Adding ICM servers to the ICM Bridge on page 286.

Configuring an additional ICM server

To configure an independent additional ICM server:

1. In IC Manager, select the **Configuration** tab.
2. From the **Tables** list in left pane, select **Chat** > **ICM**.
3. Select **New**.

4. Type a name for the additional ICM server in the **Global ICM Name** field.

   For information on all other fields, see Configuring the ICM server on page 237.

5. Click **Ok**.
6. Restart the ICM server.
7. Add the ICM server to the ICM Bridge. For more information, see Adding ICM servers to the ICM Bridge on page 286.

Adding ICM servers to the ICM Bridge

You can add ICM servers to the ICM bridge in the Attribute server configuration. For more information, see Creating the WebACD server on page 196.

To add an additional ICM server to the ICM Bridge:

1. In IC Manager, double-click the Attribute server in the list of servers.
2. Click the **Attribute** tab.
3. Click the **Ellipsis** (**…**) next to the **ICM Servers** field.
4. In the **ICM Servers** dialog box:
   a. Click **New**.
   b. Select **Enabled**.
   c. In the **Host** field, type the name and domain of the system that hosts the ICM server. For example, type TESTBOX.xyzcorp.com.
   d. Accept the default port number (9503) or change to an available port.
   e. Click **Ok**.

   Repeat these steps for each ICM server in your Avaya IC system.
5. Click **Ok**.
6. Restart the Attribute server.

Refreshing IC Manager

After you complete your Web Management configuration, refresh IC Manager and verify that the configuration information is present.

To refresh IC Manager:

1. In IC Manager, select **Manager** > **Refresh**.

2. In the **Success** message, click **Ok**.

   If you do not see a Success message, see Troubleshooting the refresh in IC Manager on page 499.

3. If required, verify that the information on the **Configuration** tab is correct.

Security configuration

Website uses Tomcat and Internet Information Services (IIS). Static requests are processed by IIS and all JSP requests are processed by Tomcat.

Configuring the required security settings for your website

1. On the IC system open the component configuration files, `server.website.xml`. The files are located at `\Avaya\IC73\tomcat\conf`.

   You can now set the required security settings in the configuration files.

2. To limit large requests to the website, configure the *`maxPostSize`* parameter.

   The *`maxPostSize`* parameter is used only to prevent large post requests with `Content-Type: application/x-www-form-urlencoded`.

   The default value of the *`maxPostSize`* parameter is 2MB. It is not necessary for you to change this value, since the website uses 2 bytes per symbol when sending a request, which means you can send 1MB of content from the website.

   Customers can also configure following tenant properties from admin website:

   - *`chat.question.maxlength`*
   - *`email.question.maxlength`*

   With these properties, customers can limit the length of questions.

3. To lower the time out value to prevent Denial-of-Service (DOS) attacks, configure the *`connectionTimeout`* parameter as follows on Tomcat and IIS:

   a. Tomcat has two connectors HTTP and AJP. You must configure the *`connectionTimeout`* parameter on both the connectors.

1. HTTP - The HTTP connector is located at port 9602. Currently *connectionTimeout* is not configured, so *connectionTimeout* takes its default value of 60 seconds, which is also the recommended value. Avaya recommends you do not set this value to a higher value as this might result in hanging your server threads for too long. On the other hand setting this value to a lower value might cause rejection of some of your requests. You must configure this value depending on the customer's environment.
2. AJP - The AJP connector is located at port 9642 (for IIS). Currently *connectionTimeout* is not configured, so *connectionTimeout* takes its default value of 60 seconds. You must syncronize the *connection_pool_timeout* parameter with the *connectionTimeout* parameter. The *connection_pool_timeout* parameter is not presented and is 0 by default, which means that idle connections are not closed. It is recommended to use values listed in Configuring Internet Information Services on page 213 and "IIS-Tomcat Redirector configuration" and "Disabling SQL Injection filter for Website" topics in the release notes.

b. To configure the *connectionTimeout* parameter on IIS, do the following:

1. Navigate to **Start** > **Internet Information Services (IIS) Manager**.
2. Select the required host, right click on requited site and the click **Manage Web Site** > **Advanced Settings** and configure the *connectionTimeout* parameter, by editing the value **Connection Time-out (seconds)** in the Connection Limits section.

   The default value of the *connectionTimeout* parameter is 120 seconds. Avaya recommends you do not change this value.

4. To configure maximum clients, maximum number of requires, and maximum threads configure the *maxThreads*, *maxConnections*, and *maxKeepAliveRequests* parameters.

a. The *maxThreads(Threads)* parameter is configured as 100. Avaya recommends you do not change this value since reducing the value of the *maxThreads* parameter leads to slow response of a system. You must configure this value based on number of a requests processed at the time in the customer's environment.

b. The *maxConnections(Clients)* parameter is not configured since IC uses BIO Tomcat mode.

c. The *maxKeepAliveRequests(Request)* parameter is not configured. The default value of *maxKeepAliveRequests* is 100 and Avaya recommends you do not change this value.

Chapter 10: Deploying CSPortal WebAPI

The CSPortal WebAPI deployment is a two-step process.

1. CSPortal WebAPI server side deployment on page 290
2. CSPortal WebAPI client side deployment on page 295

CSPortal WebAPI server side deployment

You can deploy only one website on an IC server. This website can either be the IC website or the CSPortal website. If you want to deploy both the IC website and CSPortal website, you must deploy them on different IC servers.

Note:

If you are using load balancer to route chat contact request to CSPortal server node, configure the `AIC_SESSIONID` variable on the load balancer with cookie based sticky session routing mechanism. This helps avoid the chat sessions getting disconnected due to network issues.

Prerequisite:

- Create a IC user named csportal with similar roles and priveledges as a website user
- CSPortal WebAPI must be deployed on the Secondary ORB system.

1. Run the Configure.bat file available on the IC Server.
2. In the Avaya Interaction Center Configuration Tool, click Web tab.
3. In the Web tab, provide the appropriate information for the webserver.
4. In the **Avaya Interaction Center Configuration Tool** window, on the **Web** tab, select the **Configure Web Management** option.
5. Select the **Website** option.
6. In Web Application (Website/CSPortal), select **CSPortal** from the dropdown list.
7. In the Website Virtual Directory Name, provide a name for the CSPortal site. The default name is website.
8. In the WebACD dropdown list, select WACD server name.
9. In the Attribute Server dropdown list, select the Attribute server name.
10. Select the ICM option.
11. In the **IC Login** field, provide the username for the CSPortal site.

12. In the **IC Password** field, click **...**.
13. In the **setPassword** window, provide the password for the CSPortal site.
14. In the IC Data Source field, select Interaction_Center.
15. In the Repository Data Source field, select repository.
16. In the Database Login field, provide the details of the database:
    - If the database is MS SQL, then provide username with SA credentials.
    - If the database is Oralce, then provide username with system credentials.
17. In the Database Password field, provide the password for the username specified in the above step.
18. (Optional) If you have selected MS SQL database,then select the SQL Driver (Windows Only) from the dropdown list.

    The available options are:
    - SQL Server: Select this option if you have not installed any database client on the IC Server.
    - SQL Server Native Client 10.0: Select this option if you have installed MS SQL 2008 database client on IC Server.
    - SQL Server Native Client 11.0: Select this option if you have installed MS SQL 2012 or 2014 database client on IC Server.
19. (Optional) If you have selected Oracle database, then in the Oracle Home field, provide the Oracle client location path on the IC Server.
20. Click **Apply Settings**.
21. After the settings are configured, click **Exit**.
22. From the Windows Services application, start the “Avaya IC CSPortal Web Service 7.3” service.
23. Open a browser and access the URL `http://<FQDN>:9609/csportal/v1/gettenantlist`.
24. Ensure that the browser displays a JSON formatted string listing the tenants from the IC website.

(Optional) Adding CSPortal configuration in IC Manager

The steps in Configuring the CSPortal website are optional. Do not perform these steps if the CSportal website requires only the default functionality. For example, perform these steps to create a separate csportal website when you want to have a separate debug level for the CSPortal website.

Configure dsObject parameter appropriately in `IC_INSTALL_DIR\IC73\comp\csportal\WEB-INF\web.xml`

To configure the CSPortal:

1. In IC Manager, click the **Configuration** tab.
2. From the **Tables** list in the left pane, select **Website** > **Website Context Configuration**.
3. Click **New**.
4. In the right pane, type a name for the website in the **Global Name** field.

   The CSPortal website name is case-sensitive.

   Type a name that allows you to easily identify the CSPortal website. For example, for a CSPortal website on the TESTBOX system, type **`csportal_TESTBOX`**.

   The CSPortal website uses this parameter to determine which website context record to read. This value must match the **`dsObject`** parameter in the following file on a system that hosts the website:
   `IC_INSTALL_DIR``\IC73\comp\csportal\WEB-INF\web.xml`
5. In the right pane, review the fields as shown in the following table:

Note:
Do not enter a value or change the default values in these fields unless a property needs to be explicitly changed from the default value calculated by the CSPortal website during its initialization. Most IC systems do not require changing any of these fields.

Parameter	Description
Website Debug Level	A number from 0 to 4 that represents the debug level for the website. Level 0 provides no debugging information in the logs, and level 4 provides full debugging information.
Default hostname for context	The name of the system that hosts the CSPortal website. Used by external clients to determine the location of your customer-facing website.

6. Click **Ok**.

7. Restart the Tomcat server that hosts the CSPortal Website, as shown in the following table:

Operating system	Step
Windows	From the Services Control Panel, restart the CSPortal Tomcat service.
Solaris	Run the following command: **`nohup ./ictomcat.sh start`**

Estimated Wait Time for Chat

To configure Estimated Wait Time (EWT) in the chat messages, you must enable EWT in WAA.

To enable EWT in WAA:

1. Login to IC Manager.
2. Double-click or Edit the WAA server configuration.
3. In the WAA window, click **WAA** tab.
4. In the **WAA** tab, select **Enable EWT message in Chat** option.
5. Click **Apply**.
6. Click **Ok**.
7. Restart the WAA server.

Note:
Service class EWT on CSPortal is only supported in Advocate routing.

The changes provided below is only applicable for IC 7.3.2.

- On CSPortal machine, From the Windows Services application, stop the IC Web Management service
- Open the web.xml file to edit from <Avaya Home>/comp/csportal/WEB-INF/ directory.

- In the following servlet code section, add the comment tag for the line shown in red color if you want to disable EWT status on the website. The default EWT status is set to enabled.

```
<servlet>
    <servlet-name>EWTServlet</servlet-name>
    <servlet-class>com.avaya.aic.website.service.EWTServlet</
servlet-class>
   <init-param>
<param-name>ewtenabled</param-name>
<param-value>true</param-value>
</init-param>
    <load-on-startup>6</load-on-startup>
  </servlet>
```

Security configuration for CSPortal WebAPI Server

Configuring the required CSPortal WebAPI Server security setting

1. On the IC system open the component configuration files, `server.csportal.xml`. The files are located at `\Avaya\IC73\tomcat\conf`.

   You can now set the required security settings in the configuration files.

2. To limit large requests to the website, configure the *`maxPostSize`* parameter.

   The default value of the *`maxPostSize`* parameter is 2MB. It is not necessary for you to change this value, since the website uses 2 bytes per symbol when sending a request, which means you can send 1MB of content from the website.

   Customers can also configure following tenant properties from admin website:

   - *`chat.question.maxlength`*
   - *`email.question.maxlength`*

   With these properties, customers can limit the length of questions.

   The *`maxPostSize`* parameter is used only to prevent large post requests with `Content-Type: application/x-www-form-urlencoded`.

3. To lower the time out value to prevent Denial-of-Service (DOS) attacks, configure the *`connectionTimeout`* parameter as follows on Tomcat and IIS:

   a. Tomcat has two connectors HTTP and AJP. You must configure the *`connectionTimeout`* parameter on both the connectors.

1. HTTP - The HTTP connector is located at port 9609. Currently *connectionTimeout* is not configured, so *connectionTimeout* takes its default value of 60 seconds, which is also the recommended value. Avaya recommends you do not set this value to a higher value as this might result in hanging your server threads for too long. On the other hand setting this value to a lower value might cause rejection of some of your requests. You must configure this value depending on the customer's environment.
2. AJP - The AJP connector is located at port 9699 (for Apache). Currently *connectionTimeout* is not configured, so *connectionTimeout* takes its default value of 60 seconds. You must syncronize the *connection_pool_timeout* parameter with the *connectionTimeout* parameter. The *connection_pool_timeout* parameter is not presented and is 0 by default, which means that idle connections are not closed. It is recommended to use values listed in Configuring Internet Information Services on page 213 and "IIS-Tomcat Redirector configuration" and "Disabling SQL Injection filter for Website" topics in the release notes.

4. To configure maximum clients, maximum number of requires, and maximum threads configure the *maxThreads*, *maxConnections*, and *maxKeepAliveRequests* parameters.
   a. The maximum connection pool size can be configured with the attribute *connection_pool_size* or *maxThreads(Threads)* parameter. Apache does not recommend using the *connection_pool_size* parameter with Apache httpd. For Apache httpd, IC automatically detects the number of threads per process and sets the maximum pool size to this value. For IIS, IC uses the default value of 250.

      However, if the *maxThreads* parameter configured in `server.csportal.xml` is `100`, you should not change it. You must configure this based on the customer's enviroment and depends on system loading.

   b. The *maxConnections(Clients)* parameter is not configured since IC uses the BIO Tomcat mode.

   c. The *maxKeepAliveRequests(Request)* parameter is not configured. The default value of *maxKeepAliveRequests* is 100 and Avaya recommends you do not change this value.

CSPortal WebAPI client side deployment

This deployment is similar to real world deployment where Web resources, such as JS, CSS, and images are hosted by different domain, such as CDN or Web Server in DMZ.

You can deploy CSPortal WebAPI client can be deployed on either Apache Web server, Windows IIS, or any other Web server.

- Deploying CSPortal WebAPI Client on Apache HTTP/HTTPS on page 296

- Deploying CSPortal WebAPI Client on Microsoft IIS on page 297

Deploying CSPortal WebAPI Client on Apache HTTP/HTTPS

Prerequisites:

The Apache HTTP server is installed and configured.

For more information on installing and configuring Apache HTTP server, see Apache website.

Deploying WebAPI SDK and reference implementation on Apache HTTP

To deploy WebAPI SDK and reference implementation on Apache HTTP:

1. From the IC_INSTALL_HOME\design\csportalclient directory on the IC Design & Admin system, copy the sdk and refimplementation folders to the Document Root of the Apache server.

Fom	To
<IC_Home>\design\ csportalclient\sdk	<Apache_Home>\htdocs\aic\sdk
<IC_Home>\design\ csportalclient\ refimplementation	<Apache_Home>\htdocs\aic\ refimplementation

2. Open the <Apache_Home>/conf/httpd.conf configuration file to edit.
3. In the file, remove the comment tags from the following modules:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule rewrite_module modules/mod_rewrite.so
```

4. Add the following lines at the end of the file:

```
ProxyRequestsoff
ProxyPreserveHoston
ProxyPass /csportal http://<FQDN>:9609/csportal
ProxyPassReverse /csportal http://<FQDN>:9609/csportal
```

5. Restart the Apache HTTP server.
6. Open a browser and access the URL: http://<FQDN>/aic/refimplementation/demo.html.
7. Verify that the browser displays the reference implementation shipped with the Avaya IC.

Deploying WebAPI SDK and reference implementation on Apache HTTPS

For deploying WebAPI SDK and reference implementation on Apache HTTPS see the Apache HTTPS configuration information from the Apache website.

Deploying CSPortal WebAPI Client on Microsoft IIS

About IISConfig tool

From IC 7.3.3 onwards you can configure the following using the IIS configure tool:

- CSPortal Client
- CSPortal Server
- Public Website

The ConfigIIS.bat file is located at `<IC Install Path>\IC733WinIIS\bin` folder.

This script installs the Tomcat ISAPI filter, and map it to the virtual application /aicjakarta within the website provided. The script will also create the virtual application /csportalclient mapped to `<IC_FOLDER>\comp\csportalclient` folder.

The log files of the script are stored at the following location:

`<IC Install Path>\IC733WinIIS\IC733WinIIS\bin\ConfigIIS.log`.

The command format is:

`ConfigIIS.bat <Website Name> [options]`

Here:

- Website Name is the name of the website where the application is to be deployed.

  Note:
  When providing arguments with spaces in them, for example, Default Web Site, enclose them within quotes so that they are treated as a single argument such as, "Default Web Site".

- Options are:
  - CSPC to install CSPortal Client
  - CSPS to configure CSPortal Server information
  - WS to install Public Website pages

  Note:
  The options are case insensitive. Multiple options can be specified with a space as a delimiter.

CSPC) Configure CSPortal Client: When you select CSPC) Configure CSPortal Client option, the config tool installs the CSPortal Client to the IIS website, installs Tomcat Redirector, and creates a virtual application for the CSPortal Client in IIS.

CSPS) Configure CSPortal Server: When you select CSPS) Configure CSPortal Server option, the script installs the CSPortal Server to the IIS website. You must provide Fully Qualified Domain Name of the CSPortal Server and port at which the CSPortal Server is listening. The default port is 9699. The script sets the properties in the workers.properties file located at `<IC Install Path>\IC733WinIIS\tomcat\conf\` folder.

WS) Configure Public Website: When you select WS) Configure Public Website option, the script installs the Public Websie on the IIS.

Note:
The **WS) Configure Public Website** option is not applicable for CSPortal Web API client deployment.

Deploying CSPortal WebAPI on the IIS website

CSPortal WebAPI deployment on IIS is supported from IC 7.3.3 and above.

Prerequisite:

You must add a website on Internet Information Server.

To configure the application on the IIS website:

1. Login to the server where the IIS website is configured.

2. Open Command prompt as an Administrator.
3. Go to `<IC Install Path>\IC733WinIIS\bin` folder.
4. Type **ConfigIIS.bat <Website Name>** and press **Enter**.

   The system displays the command line window with the following options:

   - CSPC) Configure CSPortal Client
   - CSPS) Configure CSPortal Server
   - WS) Configure Public Website

   Note:
   The WS) Configure Public Website option is not applicable for CSPortal Web API client deployment. For CSPortal you must use CSPC and CSPS option.
5. Type the appropriate option.
6. Follow on-screen instructions.

Deploying CSPortal WebAPI Client on IIS for IC Release 7.3.2

Pre Requisite: Before deploying CSPortal Client on the IIS, configure the appropriate roles on IIS. For details on the IIS 7.5 Web Server Role and the required services, see the Roles section in the Prerequisites for Windows 2008 Server R2 section of *Avaya IC Installation Planning and Prerequisites*.

To deploy CSPortal WebAPI Client on IIS:

1. Copy csportalclient directory from <IC Home>\design location on Design & Admin machine to the location of <IC Home>\comp on the CSPortal website machine.
2. Start IIS Manager.
3. In the **Default webSite** node, add Application.

   Alias : csportalclient

   Application Pool: DefaultAppPool

   Physical Path: <IC Home>comp\csportalclient
4. In IIS Manager, select the website that serves CSPortal Client.
5. Select **Handler Mappings** from the features grid. Click **Add** on the right pane to add a new Type.
6. Add .woff file extension and specify "application/x-font-woff" as the corresponding MIME type.
7. Re-start the IIS server.

Deploying WebAPI SDK and reference implementation on Microsoft IIS with HTTPS

For deploying WebAPI SDK and reference implementation on Microsoft IIS with HTTPS see the Microsoft IIS documentation on HTTPS configuration from the Microsoft website.

Removing DWSensor plugin from IIS

DWSensor plugin is used for DataWake feature on the public website. The DWSensor is automatically installed when you deploy a website or CSPortal even if the feature is not used.

Remove DWSensor if not used.

To remove DWSensor plugin in IIS7.x on Microsoft Windows 2008 R2 or Microsoft Windows 2012 server:

1. Open the Internet Information Services (IIS) Manager.
2. Click the website node where Avaya IC website is deployed. For example, the default website.
3. In the home page of the website, double-click ISAPI filters node.
4. Select DWSensor plugin from the list. Right-click on the DWSensor plugin and click Remove.
5. Restart IIS Server website.

Security configuration for CSPortal WebAPI Client

Configuring the required CSPortal WebAPI Client security setting

1. On the IC system open the Apache httpd file, which is called `httpd.conf`. The httpd.conf file is located at `\Apache Software Foundation\Apache2.2\conf`.

   You can now set the required security settings in the `httpd.conf` file.
2. To limit large requests to the website, configure the following parameters.
   - *`LimitRequestLine`*. This parameter is set to its default value, which is `8190`.
   - *`LimitRequestBody`*. This parameter is set to its default value, which is `0`.
   - *`LimitXMLRequestBody`*. This parameter is set to its default value, which is `1000000`.

   These parameters does not have any effect when emails or chats are sent from CSPortal UI, however these parameters can be used to prevent different attacks based on large requests.

3. To lower the time out value to prevent Denial-of-Service (DOS) attacks, configure the following directories:
   - *KeepAlive*. This parameter is set to its default value, which is `On`.
   - *KeepAliveTimeout*. This parameter is set to its default value, which is `5`.
   - *Timeout*. This parameter is set to its default value, which is `60`.
   - *ProxyTimeout*. This parameter is set to its default value, which is `60`.

   You must configure these parameters based on value depending on the customer's environment and system loading. Avaya recommends using the default values.

   The following property must also be configured:

   ```
   ProxyPass/csportal http://win37101.mera.ru:9609/csportal
   connectiontimeout=5 timeout=30
   ```

4. To configure maximum clients, maximum number of requests, and maximum threads configure the following parameters:
   - *StartServers*
   - *MinSpareServers*
   - *MaxSpareServers*
   - *MaxClients*
   - *MaxRequestsPerChild*

   You must configure these parameters based on value depending on the customer's environment and system loading.

Uninstalling CSPortal

Prerequisites

Shut down the IC website.

To uninstall CSPortal:

1. Run the Configure.bat file available on the IC Server.
2. In the Avaya Interaction Center Configuration Tool window, on the **Web** tab, select the **Configure Web Management** option.
   - Clear Website option.

   Or

   - Select the **Website** option and in the **Web Application (Website/CSPortal)** option, select **Website** from the drop-down list.

3. Click **Apply Settings**.
4. After the settings are configured click **Exit**.
5. If you have selected to deploy IC website, then from Windows Services application, start the IC Web Management service.
6. Open a browser and access the URL: http://<FQDN>/website/public.
7. Ensure that the browser displays the IC public website.

Chapter 11: Configuring IC Websites over HTTPS

This chapter describes how to configure IC websites over the HTTPS protocol using self-signed certificates.

This chapter includes the following topics:

- Configuring SSL on Windows on page 304
- Configuring SSL on Solaris on page 313
- Configuring SSL on AIX on page 319

Before you configure SSL

Before you configure Web Management or Email Management to use SSL, perform the following steps and install and configure SSL:

1. Generate SSL authentication keys and a certificate request.
2. Submit the certificate request to a certifying authority, such as VeriSign, Thawte, or your own internal enterprise CA.
3. Import the signed certificate and configure the Web server to use the signed certificate returned by the certifying authority.

Note:

For production systems, the customers must get the certificates from a certifying authority only.

Configuring SSL on Windows

Before you configure SSL on the Windows platform, it is assumed that the IC Website [public/admin] is successfully installed and configured and is accessible over the http protocol. For more information, see Chapter 9: Configuring Web Management on page 194.

Ensure that you have the following:

- The ICM server is in stopped state.

- The Attribute server is in stopped state.
- The IC Website server is in stopped state.

If CIRS is configured, all the website servers must be configured for https. The procedure for configuring https is explained for one website server only.

Reconfiguring website using the IC configure tool

To reconfigure the website using the IC configure tool:

1. Rerun the IC configure tool on the server where website is configured.
2. Enter port number as 443 and click **Apply Settings**.
3. Click **Exit**.

Generating an IIS self-signed certificate

You can create self-signed certificate within the IIS 7 administration console. SSL certificates enable the encryption of all traffic sent to and from your IIS website, preventing others from viewing sensitive information. It uses public key cryptography to establish a secure connection. This means that anything encrypted with a public key (the SSL certificate) can only be decrypted with the private key and vice versa.

When you try to connect to an IIS website that uses a self-signed certificate, you see the security certificate warning message until you store the certification in the certificate store on your system.

To generate an IIS self-signed certificate:

1. Go to the Windows Run (Windows key + R) and type `intermgr.exe` command and enter.

   The IIS 7 administration console opens.
2. Double-click the **Server Certificates** icon.
3. In the **Actions** column on the right, click **Create Self-Signed Certificate....**
4. Type any name and click **OK.**

   You will now have an IIS self-signed certificate valid for 1 year listed under Server Certificates. The certificate common name (Issued To) is the server name.

Binding the self-signed certificate

To bind the self-signed certificate:

1. In the **Connections** column on the left, expand the sites folder and click the website that you want to bind the certificate to. (It is the default website in this case).
2. Click **Bindings...** in the right column.
3. Remove http type binding.
4. Click **Add...**
5. Select the type https and select the self-signed certificate. Click **OK**.

   You can now see the binding for port 443 listed. Ensure that port 80 binding is removed. For https binding only port 443 must be configured for the AIC website.
6. Click **Close**.

Note:
Do not configure both http and https binding on IIS. IC Web Applications (such as RLManager, Admin/Public Website, and so on) might not work properly when both http and https are configured on IIS.

After you have bound the new certificate to your IIS site, visit the certificate with https in your web browser and the system displays the following error:

"The security certificate presented by this website was not issued by a trusted certificate authority."

This is a normal error for self-signed certificates, because the certificate is signed by itself instead of a trusted SSL provider. All visitors to the site see the error, unless they import the self-signed certificate into their Trusted Root Certification Authorities store (or the appropriate SSL certificate store for the browser they are using). You can easily add the IIS self-signed certificate to the store on the server by following the instructions below. If you need to import the certificate on another Windows machine, just follow the instructions on how to Move or copy an SSL certificate from a Windows server.

Adding the self-signed certificate to Trusted Root Certificate Authorities

To add the self-signed certificate to the Trusted Root Certificate Authorities store:

1. Click on the **Start > Run**.
2. In the **Open:** field, type **mmc** and click **OK**.
3. Click the **File** menu and click **Add/Remove Snap-in**...
4. Double-click **Certificates**.

5. On the Certificates snap-in page, select **Computer Account** and click **Next**.
6. Click **Finish**.
7. Expand the Certificates item on the left and expand the Personal folder. Click the Certificates folder and right-click the self-signed certificate that you just created and select **Copy**.
8. Expand the Trusted Root Certification Authorities folder and click the Certificates folder under it.
9. Right-click in the white area below the certificates and click **Paste.**

   The error that the system displayed earlier is resolved.

Editing webadmin configuration file

To edit the configuration file, you must perform the following steps on the machine where the IC Admin website is configured:

1. In Notepad or another text editor, open the `webadmin.cfg` file from the `\Avaya\IC73\etc` directory.
2. Change the value of the **serverPort** attribute to `443`.
3. Change the value of the **protocol** attribute to `https`.
4. Save and close the file.

Modifying the website configuration

You must add/modify an existing website configuration to use SSL values.

To modify the website configuration:

1. In IC Manager, select the **Configuration** tab.
2. From the Tables list in left pane, select **Website > Website Context**.
3. In the right pane, select the entry for the website and click **Edit**. If there is no existing entry governing website configuration, then add a new one.
4. From the **Default internet protocol** drop-down list, select https.
5. In the **Default port for context** field, type `443`.
6. Click **Ok**.
7. Select **Manager > Refresh**.

Configuring the WebACD server

To configure the WebACD server:

1. In IC Manager, double-click the **WebACD server**.
2. Click the **WACD tab**.
3. In the **WACD Webserver** field, update the appropriate values.
4. In the **Ports** field, type `443`.
5. In the Protocol drop-down list, select **https://**
6. Click **OK.**
7. Restart the WACD server for it to update the properties correctly.

Note:

Repeat the above procedure for the secondary WACD server that is part of the WACD cluster configuration. The WACD Webserver host name that needs to be specified for both the primary and secondary WACD servers is the hostname where the website's webserver is hosted over which WACD services can be accessed via https.

The above settings are used for the following:

- Used by the IC Admin site to configure URLs for the WACD access.
- Used as Agent Home Address URL, part of the Web Agent Desktop.

Modifying the SSL properties

To modify the SSL properties:

1. In IC Manager, select **Tools** > **Groups**.
2. Select the **Properties** tab.
3. Select IC in the left pane of the Group Manager.
4. Select **System/Configuration** in the Sections list.
5. Click **Edit** and set values for the properties, as shown in the following table:

Property	Recommended entry
ChatLoginServerProtocol	https
ChatLoginServerPort	443
ChatLoginServer	Website webserver's hostname

6. Click **Ok**.
7. Exit the IC Manager Administration Console.

Exporting the CA certificate

To export CA certificate:

1. Click on the **Start > Run**.
2. In the Open field, type `mmc` and click **OK**.
3. Click on the **File > Add/Remove Snap-in**...
4. Double-click **Certificates**.
5. Select **Computer Account** and click **Next.**
6. Leave Local Computer selected and click **Finish**.
7. Click **OK**.
8. Click the plus sign next to Certificates in the left pane.
9. Click the plus sign next to Trusted Root Certification Authorities and click the **Certificates** folder.
10. Select the certificate to be exported in the right-pane.
11. Click **Action > All Tasks** and then **Export**.
12. In the Certificate Export Wizard, click **Next**.
13. Select **No, export the private key** and click **Next**.
14. Select **DER encoded binary X.509 (.CER)** and click **Next**.
15. Browse to the appropriate directory location and type a name of the certificate.
16. Click **Finish**. The .cer file containing the root certificate is now saved to the location you specified.

About importing the CA certificate

You must import the CA certificate to other machines from where public/admin website would be accessed. You must perform this activity on the following machines:

- Machine from where IC admin site is accessed over SSL
- On all the machines where Agent desktops are installed or accessed.
- On test machines used for public website testing.
- IC Manager server from where various IC Admin website functionalities can be accessed.

This procedure is not required in case the CA root authority is a trusted certifying authority such as VeriSign or Thawte that has signed the server certificate. This procedure is required only if you need to always trust the self-signed server certificate and prevent any kind of browser warning.

Importing CA certificate in the Windows MMC console

Note:
Before you import the certificate, copy the exported certificate to the system where it will be imported.

To import CA certificate in the Windows MMC console:

1. Click on the **Start menu > Run**.
2. In the Open field, type `mmc` and click **OK**.
3. Click **File** and then click **Add/Remove Snap-in**...
4. Double-click on Certificates.
5. Click **Computer Account** and then click **Next**.
6. Leave Local Computer selected and click **Finish**.
7. Click **OK**.
8. Click the plus sign next to Certificates in the left pane.
9. Click the plus sign next to Trusted Root Certification Authorities and click the **Certificates** folder. Right Click, All Tasks and then **Import**…
10. In the **Certificate Import Wizard**, click **Next**.
11. Click **Browse** and select the .cer extension file which has the CA root certificate that you copied over, and click **Open** and then **Next**.
12. Click the **Place all the certificates in the following store**:**Trusted Root Certification Authorities** option**.**
13. Click **Next**.
14. Click **Finish** to complete the wizard.

    The certificate is now listed as one of the trusted root certificate.
15. Close the MMC console.

Importing the CA certificate in the JAVA Keystore on server machine where IC Manager is configured

This is an additional step which needs to be carried out on the IC Manager server. The CA root authority certificate also needs to be imported in the Java keystore i.e. in the IC Manager used JRE's database of trusted certificates.

This allows IC Manager to trust the certificate coming from IC website server during SSL handshake. The following steps install the signing authority (CA) credentials, which has signed the certificate of IC website server, and used JRE's database of trusted certificates of the IC Manager system.

For the above, the certificate imported in the "Trusted Certification Store" has now to be exported in the .X09 format.

Note:

Before you import the certificate, copy the exported certificate to the system where it will be imported.

To import the CA certificate in JAVA Keystore:

1. Copy the IC websites CA's certificate from IC website server machine to IC Design & Admin machine's on %AVAYA_IC73_HOME%\Java\lib\security folder. File name is of type "*.cer".
2. Open the command prompt and run the following commands to import above certificate:
    1. cd %AVAYA_IC73_HOME%\Java\lib\security.
    2. "%AVAYA_IC73_HOME%\Java\bin\keytool.exe -import -file <the exported certificate name>.cer

        -alias <Certificate Unique Alias Name> -keystore jssecacerts -storepass changeit
3. When prompted to trust the certificate, click **Yes**.
4. Verify that the jssecacerts keystore has successfully imported the CA certificate by checking the output of the following command:
    - %AVAYA_IC73_HOME%\Java\bin\keytool.exe -list -v -alias <Certificate Alias Name> -keystore jssecacerts -storepass changeit.

Note:

The default password for `jssecacerts` keystore is **changeit**. Use the appropriate password if it is changed. All keystore entries (key and trusted certificate entries) are stored and accessed using unique, case-insensitive aliases through the keystore. If certificate alias name is not provided, then the default alias name mykey is be used by the keytool.

Importing the CA certificate in the JAVA Keystore on server machine where Website and ICM are configured for SSL SMTP

This is an additional step which needs to be carried out on the IC Website and ICM. The CA root authority certificate also needs to be imported in the Java keystore i.e. in the IC Website and ICM used JRE's database of trusted certificates.

This will allow IC Website and ICM to trust the certificate coming from IC website server during SSL handshake. The following steps will install the signing authority (CA) credentials, which has signed the certificate of IC website server, and used JRE's database of trusted certificates of the IC Website and ICM.

For the above, the certificate imported in the "Trusted Certification Store" has now to be exported in the .X09 format.

Note:

Before you import the certificate, copy the exported certificate to the system where it will be imported.

To import the CA certificate in the JAVA Keystore on server machine where Website and ICM are configured for SSL SMTP:

1. Copy the IC websites CA's certificate from IC website server machine to IC core server machine's on %AVAYA_IC73_HOME%\Java\lib\security folder. File name is of type "*.cer".
2. Open the command prompt and run following commands to import above certificate:
   a. cd %AVAYA_IC73_HOME%\Java\lib\security.
   b. "%AVAYA_IC73_HOME%\Java\bin\keytool.exe -import -file <the exported certificate name>.cer

      -alias <Certificate Unique Alias Name> -keystore jssecacerts -storepass changeit
3. When prompted to trust the certificate, click **Yes**.
4. Verify that the jssecacerts keystore has successfully imported the CA certificate by checking the output of following command:
   - %AVAYA_IC73_HOME%\Java\bin\keytool.exe -list -v -alias <Certificate Alias Name> -keystore jssecacerts -storepass changeit.

Note:

The default password for `jssecacerts` keystore is **changeit**. Use the appropriate password if it is changed. All keystore entries (key and trusted certificate entries) are stored and accessed using unique, case-insensitive aliases through the keystore. If certificate alias name is not provided then the default alias name mykey will be used by the keytool.

Starting the IC Website, ICM, and Attribute Servers

To start the IC website, ICM, and Attribute servers:

1. Log on to the website server machine where the IC website is configured and start all the IC chat servers.
2. Open the Windows services window and start the following set of chat servers.
   - CIRS server (if configured): Avaya IC CIRS Service 7.3
   - ICM server: Avaya IC ICM Service 7.3
   - IC Website server: AvayaICWebManagement73
3. Re-log in to the IC Manager Administration console and start the Attribute server.

   You can now access the IC public/admin website over https.

   You can now access the WACD, Web Response Unit and Multitenant administration functionalities over https via IC Manager.

Configuring SSL on Solaris

For the prerequisites for configuring SSL on Solaris, see Before you configure SSL on page 304

Reconfiguring the website using IC configure tool

To reconfigure the website using the IC Configure tool:

1. Rerun the IC Configure tool on the server where the website is configured.
2. Enter the Web server port as: 443 and click **Apply Settings**.

Note:

When you apply the settings, you can agree for deploying and pulling the configuration changes to the iPlanet webserver config store. Alternatively, you can do this externally using the iPlanet webserver administration console.

Creating and installing the self-signed certificate in iPlanet

Note:

For the set of commands listed in this procedure, the following attributes needs to be provided based on the actual host name and their organization details of the customer.

These attributes must be provided by the customer as applicable: config (which was used for HTTP), org-unit, state, validity, or, country, server-name, and nickname.

To create and install the self-signed certificate in iPlanet:

1. Navigate to <iplanet_home_dir> and create a file by name admin.pwd. This file contains the iPlanet administrator password. An example is as follows:

   wadm_password=admin

2. Navigate to the iPlanet bin directory, where the "wadm" tool is located: <iplanet_home_dir>

   The following command will create the self-signed certificate:

   ```
   ./wadm create-selfsigned-cert --user=admin --port=8989
     --password-file=../admin.pwd --config=puicdevsol09
     --token=internal --org-unit=cc --locality=denver --state=co
     --validity=24 --org=avaya --country=US
     --server-name=puicdevsol09.rnd.avaya.com --nickname=sol09certSSL
   ```

   Command response: `CLI201 Command 'create-selfsigned-cert' ran successfully.`

3. Type the following command to list the self-signed certificate just created:

   ```
   ./wadm list-certs --user=admin --password-file=../admin.pwd
     --host=puicdevsol09.rnd.avaya.com --port=8989 --ssl=true
     --prompt=false --rcfile=null --config=puicdevsol09
   ```

   Command response: `sol09certSSL`

4. Type the following command to create an SSL enabled HTTP listener port in the iPlanet webserver.

   ```
   ./wadm create-http-listener --user=admin --password-file=../
     admin.pwd host=puicdevsol09.rnd.avaya.com --port=8989
     --listener-port=443 --config=puicdevsol09
     --server-name=puicdevsol09.rnd.avaya.com
     --default-virtual-server-name=puicdevsol09 http-listener-ssl
   ```

   Command response: `CLI201 Command 'create-http-listener' ran successfully`

   The above command creates a new listener by name http-listener-ssl for listening https webserver request.

5. Type the following command to enable the newly created listener for SSL in the previous step:

   ./wadm set-ssl-prop --user=admin --password-file=../admin.pwd --config=puicdevsol09 --http-listener=http-listener-ssl enabled=true

   Command response: CLI201 Command 'set-ssl-prop' ran successfully

6. The following command associates the HTTP listener port with the nick name of the self-signed certificate:

   ./wadm set-ssl-prop --user=admin --password-file=../admin.pwd --config=puicdevsol09 --http-listener=http-listener-ssl server-cert-nickname=sol09certSSL

   Command response: `CLI201 Command 'set-ssl-prop' ran successfully`

7. The following command deploys the modified configuration:

   ./wadm deploy-config --user=admin --password-file=../admin.pwd --host=puicdevsol09.rnd.avaya.com puicdevsol09

   puicdevsol09 above is the iPlanet configuration name.

   Command response: `CLI201 Command 'deploy-config' ran successfully.`

8. Log in to the iPlanet administration console by entering https://puicdevsol09.rnd.avaya.com:8989/admin.

Note:
The Admin port and the hostname change according to your configuration.

9. On the Home page, select the appropriate configuration, and then click **Edit Configuration**.
10. Ensure that there are no pending deployment changes that need to be pulled into the config store.
11. If there are any deployment changes pending, then complete this activity and click **OK** if the changes are acceptable.
    a. On the **Edit Configuration** page, click **Instance Configuration Modified**. The system displays the **Configuration Deployment** page.
    b. Select **Pull and deploy configuration from**.
    c. Click **OK**. The system displays a message: The configuration has been deployed successfully to all available nodes.
12. Click the **Http Listeners** tab.
13. Now select the listener configured on a port for http-requests.
14. Click the **Delete** button.
15. Click **OK** to delete the listener.

    Deleting puts the instance in Deploy pending mode.

16. Click the **Deployment Pending** as seen on the upper right corner and click **Deploy** to deploy the configuration changes.
17. Click **Home** and click the **Configurations** tab.
18. Select the appropriate instance and click **Start**.
19. Go to the browser and type in the URL appropriate to your web server and port number as 443. The system might display the error message There might be a problem with this website's security certificate.

Note: **July 2021**

This is a normal error for self-signed certificates, because the certificate is signed by itself instead of a trusted SSL provider. All visitors to the site see the error, unless they import the self-signed certificate into their Trusted Root Certification Authorities store or the appropriate SSL certificate store for the browser they are using.

About exporting and importing a server self-signed certificate

This procedure is not required in case the CA root authority is a trusted certifying authority, such as VeriSign or Thawte that has signed the server certificate. This procedure is required only in case one wants to always trust the self-signed server certificate and prevent any kind of browser warning.

Export and import must be performed on the following machines:

- Machine from where IC admin site is accessed over SSL.
- On all the machines where Agent desktops are installed or accessed.
- On test machines used for public website testing.
- On IC Manager server from where various IC Admin website functionalities can be accessed.

Exporting and importing a server self-signed certificate

To export and import a server self-signed certificate:

1. Log in to the IC webserver machine and traverse to the webserver installation directory bin folder: <iplanet_home_dir>.
2. Type the following command: **`pk12util -o /tmp/puicdevsol09.p12 -n sol09certSSL -d../https-puicdevsol09/config`**. This command exports the self-signed certificate puicdevsol09.p12 in the (PKCS12) format in the tmp directory.

Note:

The certificate name and the certificate directory vary according to the customer's configuration. In the previous step, the certificate name is sol09certSSL, the certificate directory is https-puicdevsol09/config.

3. Enter the appropriate password, which will be used during the import operation.

Note:
After the previous step, the certificate/key is exported and stored with an extension of .p12 in the /tmp directory. This file is now ready to be imported on to the Windows machine, where IC website application would be accessed.

Importing the self-signed certificate

To import the self-signed certificate:

1. Click **Start >Run**.
2. In the **Open:** field, type **mmc** and click **OK**.
3. Click on the File menu and click **Add/Remove Snap-in**...
4. Double-click **Certificates**.
5. Click **Computer Account > Next**.
6. Leave Local Computer selected and click **Finish**.
7. Click **OK**.
8. Click the plus sign next to Certificates in the left pane.
9. Click the plus sign next to Trusted Root Certification Authorities and click the **Certificates** folder. Right-click **All Tasks > Import**…
10. In the **Certificate Import Wizard**, click **Next**.
11. Click **Browse** and select the .p12 extension file which has the CA root certificate that you copied over and click **Open** and then click **Next**.
12. Follow the application wizard to complete the rest of the steps for Importing the certificate into the Trusted Root certification store.
13. Enter the admin password for the certificate to be imported. Click **Next**.
14. Select Place all certificates in the following store, and Browse to Trusted Root Certification Authorities.
15. Click **Next**.
16. Click **Finish**. The system displays a message that the certificate import was successful.
17. Open the Internet Explorer browser and test the IC Webserver URL configured for https access. It should show the Oracle iPlanet home page without any certificate error.

Editing the configuration file

To edit the configuration file:

1. In Notepad or another text editor, open webadmin.cfg.

2. Change the value of the attribute serverPort to 443.
3. Type `https://` as the protocol.
4. Save and close the file.

Modifying the website configuration

To modify the website configuration:

1. In IC Manager, click the **Configuration** tab.
2. From the **Tables** list in left pane, select **Website > Website Context**.
3. In the right pane, select the entry for the website and click **Edit**. If there is no existing entry governing website configuration, then add a new one.
4. From the **Default internet protocol** drop-down list, select **https**.
5. in the **Default** port for context field, type 443.
6. Click **Ok**.
7. Select **Manager > Refresh**.

Configuring the WebACD server

To configure the WebACD server:

1. In IC Manager, double-click the WebACD server in the lists of servers.
2. Click the **WACD** tab.
3. In the WACD Webserver field, update the appropriate values.
4. Click **OK**.
5. Restart the WACD server for it to update the properties correctly.

Note:

Repeat the above procedure for the secondary WACD server that is part of the WACD cluster configuration. The WACD Webserver host name that needs to be specified for both the primary as well as secondary WACD servers is the hostname where the website's webserver is hosted over which WACD services can be accessed via https. The above settings are used for following:

- Used by the IC Admin site to configure URLs for the WACD access.
- Used as Agent Home Address URL, part of the Web Agent Desktop.

Modifying the Group SSL properties

To modify the group SSL properties:

1. In IC Manager, select **Tools > Groups**.
2. Select the **Properties** tab.
3. Select **IC** in the left pane of the Group Manager.
4. Select **System/Configuration** in the Sections list.
5. Select Edit and set values for the following properties:

Property	Recommended entry
ChatLoginServerProtocol	https
ChatLoginServerPort	443
ChatLoginServer	Website webserver's hostname

6. Click **Ok**.
7. Exit the IC Manager Administration console

For further steps on this procedure, see Reconfiguring website using the IC configure tool on page 305.

Configuring SSL on AIX

For prerequisites to configure SSL on AIX, see Before you configure SSL on page 304.

Reconfiguring Website using IC configure tool

To reconfigure the website using the IC configure tool:

1. Rerun the IC configure tool on the server where website is configured.
2. Enter the Web server port as: 443 and click **Apply Settings**.

Creating and configuring Self-Signed Certificate in IHS

To create and configure self-signed certificate in IHS:

1. Log in to the AIX server machine with the username which was used for IHS webserver installation.
2. Add the IHS websever jre bin directory to the "PATH" environment variable.
3. Export PATH=<ihs_install_directory>/java/jre/bin:$PATH
4. Launch ikeyman tool from following location: <ihs_install_directory>/bin/ikeyman OR /usr/IBM/HTTPServer1/bin/ikeyman in this case.
5. Create a Key database. A key database is a file that the server uses to store one or more key pairs and certificates.
6. Click **key database file** from the main user interface, then click **New**. Select **CMS** for the Key database type. IBM HTTP Server does not support database types other than CMS. Now enter the details like File Name and Location for storage. Click **OK**.
7. Enter your password in the Password Prompt dialog box, and confirm the password.
8. Select **Stash the password to a file**. Click **OK**.

   The new key database should display in the ikeyman utility with default signer certificates. Ensure that there is a functional, non-expiring signer certificate for each of your personal certificates.

   The key database file has been created by name as "key.kdb" in the following location: /<ihs_install_directory>/KeyDB directory.

   Note:
   ikeyman provides the functionality to create self-signed certificate to enable SSL sessions between client and server. The self-signed certificate which would be created would be stored in the key.kdb database created in the previous step.
9. Click **Personal Certificates** in the Key Database content frame, and click the **New Self-Signed** button.
10. Enter the following information in the Password Prompt dialog box:
    - Key label: Enter a descriptive comment to identify the key and certificate in the database.
    - Version: Select the appropriate version.
    - Key size: Choose your level of encryptions from the drop-down menu.
    - Signature Algorithm: Select the appropriate algorithm.
    - Common Name: Enter the fully qualified host name of the Web server as the common name. Example: icsvaixoa02.rnd.avaya.com
    - Organization Name: Enter your organization name.

- Optional: Organization Unit
- Optional: Locality
- Optional: State/Province
- Optional: Zip code
- Optional: Country or region
- Validity Period

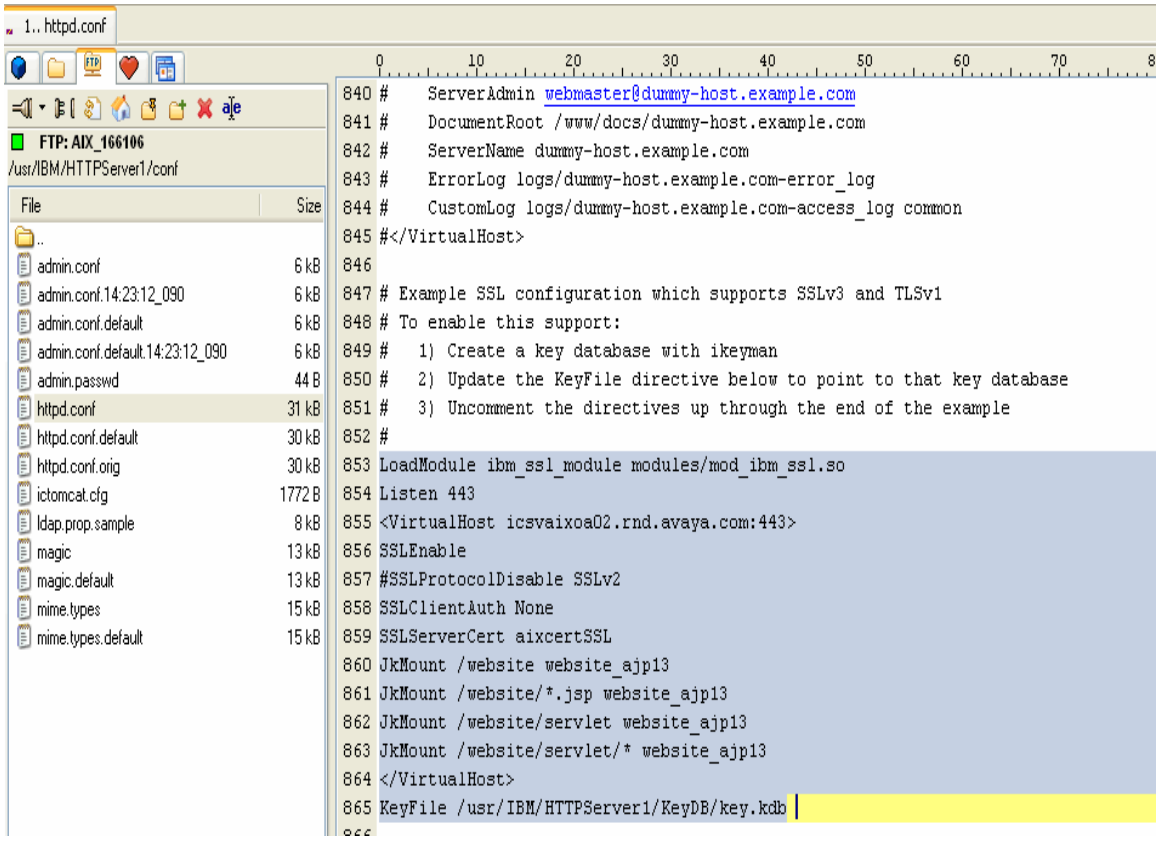
11. Click **OK**.
12. Exit the ikeyman tool.

Configuring the IHS httpd.conf file

To configure the IHS httpd.conf file:

1. Open the <ihs_install_directory>/conf/httpd.conf file.
2. Disable the http Listener configured at port 80 as follows:
   - Old Value: Listener:80
   - New Value: #Listener:80

3. Enable the SSL configuration as shown in the image. Modify the following lines as shown in the image. In the image, website is assumed to be the context name.



4. Save and close the file.
5. Start the IHS server. ***IC_INSTALL_DIR*/IC73/bin/httpserver.sh start**.

   You can now access the IHS server over https protocol as follows: https://<webserver>:443.

Note:

This is a normal error for self-signed certificates because the certificate is signed by itself instead of a trusted SSL provider. All visitors to the site will see that error unless they import the self-signed certificate into their Trusted Root Certification Authorities store or the appropriate SSL certificate store for the browser they are using.

Problems encountered before exporting the certificate

The system displays the following error message: The command cannot complete because your JRE is using restricted policy files. The reason for this error is restricted JCE policy files.

To resolve the problem, perform the following steps:

1. Download and install the files from the Unrestricted JCE policy files site.
2. Rename and move the restricted -local_policy.jar, and -US_export_policy.jar JCE Policy files from the <ihs_install_directory>/java/jre/lib/security/ directory to a directory that is outside the JDK class path, extdirs, or bootclasspath.
3. Place the unrestricted JCE policy files in the <ihs_install_directory>/java/jre/lib/security/ directory. Name the local_policy.jar and US_export_policy.jar.
4. Restart the ikeyman utility to pick up the unrestricted JCE policy files now located in the security directory.

Exporting keys to a PKCS12 file

To export keys ro a PKCS12 file:

1. Navigate to the <ihs_install_directory>/bin directory location of the AIX IHS webserver.
2. Enter ikeyman on a command line to start the Export utility.
3. Click **Key Database File** from the main UI, then click **Open**.
4. Enter your key database name in the Open dialog box, or click key.kdb if you use the default. Click **OK**.
5. Enter your password in the Password Prompt dialog box, and click **OK**.
6. Click **Personal Certificates** in the Key Database content frame. Click the certificate.
7. Click **Export/Import**.
8. In the **Export/Import Key** window:
   a. Click **ExportKeyM**.
   b. Choose **PKCS12** as the Key file type.
   c. Enter the file name, or use the Browse option.
   d. Enter the correct location.
9. Click **OK**.
10. Enter the correct password in the Password prompt dialog box, and enter the password again to confirm. Click **OK** to export the selected key to a PKCS12 file.

Note:

After the previous step, the certificate/key would be exported and stored with an extension of .p12 in the above directory specified by Location attribute. This file is ready to be imported on to the Windows machine where IC website application would be accessed.

Importing Keys (.p12) to the Windows Trusted Stored in Windows 7

To import keys to the Windows Trusted stored in Windows 7:

1. Click **Start** to open Certificate Manager.
2. Type certmgr.msc into the search box, and press **Enter**. Administrator permission required If you're prompted for an administrator password or confirmation, type the password or provide confirmation.
3. Click the folder that you want to import the certificate into, click the **Action menu> All Tasks**.
4. Click **Import**.
5. Click **Next**, and then follow the instructions.

   The certificate is imported successfully.
6. Open the Internet Explorer browser and test the IC Webserver URL configured for https access. It should show the IHS home page without any certificate error.

Editing webadmin configuration

For procedure on editing the webadmin configuration file, see Editing webadmin configuration file on page 307.

Modifying the Website configuration

For procedure on modifying the website configuration, see Modifying the website configuration on page 307.

Configuring the WebACD server

For procedure on configuring the WebACD server, see Configuring the WebACD server on page 308.

Modifying the SSL properties

For procedure on modifying the SSL properties, see Modifying the SSL properties on page 308

Exporting the CA certificate in the JAVA Keystore

To export the CA certificate in the JAVA Keystore:

1. Click **Start > Run**.
2. Type in `mmc` and click **OK**.
3. Click on the File menu and click **Add/Remove Snap-in...**

4. Add "Certificates" as the standalone snap-ins to the "Computer account" of the Local Computer.
5. Click on the certificate which was imported from the Solaris iPlanet server. Select **Action > All Tasks > Export...**
6. Choose **DER encoded binary X.509 (.CER)** and click **Next**.
7. Choose a file name with extension .cer on to a local drive where the certificate would be exported.
8. Click **Finish**.

   The .cer file containing the root certificate is now saved to the location you specified.
9. Copy the IC websites CA's certificate from IC website server machine to IC Design & Admin machine's on %AVAYA_IC73_HOME%\Java\lib\security folder. File name is of type "*.cer". "puicdevsol09.cer", in this particular case.
10. Verify that the jssecacerts keystore has successfully imported the CA certificate by checking the output of following command:

    "%AVAYA_IC73_HOME%\Java\bin\keytool.exe -list -v -alias <Certificate Unique Alias Name> -keystore jssecacerts -storepass changeit.

Note:

The default password for jssecacerts keystore is changeit. Use the appropriate password if it is changed. "All keystore entries (key and trusted certificate entries) are stored and accessed via unique, case-insensitive aliases through the keystore. If certificate alias name is not provided then default alias name mykey will be used by keytool.

Starting the IC Website, ICM and Attribute Servers

To start the IC website, ICM, and Attribute servers:

1. Log on to the website server machine where IC website is configured and start all the IC chat servers.
2. Navigate to the $AVAYA_IC73_HOME/bin directory and start the following chat related servers:
   a. CIRS server (if configured): nohup ./cirs.sh start.
   b. CM chat server: nohup ./icm.sh start.
   c. IC website server: nohup ./ictomcat.sh start website.
3. Re-login to the IC Manager Administration console and start the "Attribute server".

   You can now access the IC public/admin website over https.

You can now access the WACD, Web Response Unit and Multitenant administration functionalities over https via IC Manager.

Chapter 12: Configuring Email Management

Email Management is part of the email channel for IC.

To configure Email Management, perform the steps in the following topics:

1. Before you configure Email Management on page 327
2. Configuring an IC Poller Server on page 327
3. Configuring an IC Email server on page 329
4. Configuring Email Template Administration on page 333
5. Configuring a Workflow server for Email Management on page 342
6. Using workflows for Email Management on page 348
7. Creating routing hints for email workflows on page 350
8. Configuring the WebACD server for Email Management on page 352
9. Integrating Email Template Administration on page 353
10. Configuring email accounts on page 354
11. Creating an email status on page 367
12. Configuring Avaya Content Analyzer (optional) on page 368

Your IC system can also include optional Email Management features, such as an approval process or email message loop detection. For more information on how to configure these features, see *Interaction Center Administration Guide*.

Tip:
For information on how to set up RONA for Email Management, see *Interaction Center Administration Guide*.

Before you configure Email Management

Before you configure Email Management, you must:

1. Verify that all the required third party software, including SMTP servers, POP3 servers, IMAP4 servers, and email accounts are installed and configured and are accessible through the network. For more information, see *Avaya IC Installation Planning and Prerequisites*.
2. Copy the IC server files to the target systems, as described in Installing IC server components on page 35.
3. Configure a secondary server environment, as described in Configuring the ORB server environment on page 44.
4. Perform all the steps to configure the IC servers, databases, and related components, described in Configuring core servers on page 83.
5. Configure Web Management, as set out in Configuring Web Management on page 194.

Configuring an IC Poller Server

The Poller server interacts with POP3, and IMAP4 servers, polls emails from the exchange server that you have configured, and stores them in a database.

This section includes the following topics:

- Guidelines for IC Poller Server on page 327
- Creating the IC Poller Server on page 327

Guidelines for IC Poller Server

Ensure that the failover strategy for your IC domains includes the following:

- A domain should contain only one Poller server.

Creating the IC Poller Server

The IC installation program does not automatically add the Poller server. Email Management requires this server for polling the mails from the exchange server.

To create the IC Poller Server:

1. In the IC Manager, select **Server** > **New**.
2. From the list of server types, select **Poller** and click **Ok**.
3. On the **General** tab, enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	Poller_<*domain*>	To identify the server, include the domain in the server name.
Domain	IC.	For example, select `Poller` from the drop-down list if the server is in the Poller domain.
Host	IP address of the Poller server	When you select the host, IC Manager fills the fields for Directory, Port, and Executable.

4. Click the **Poller** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
IC Data Source	Interaction Center Data Source.	The default data source name is: `interaction_center`.
Maximum Messages Retrieved per POP3 Cycle	240	Determines the maximum number of email contacts retrieved from a POP3 or IMAP4 server over a single connection.
POP3 Cycle Wait Time (sec)	240	Specifies the default number of seconds that the server waits between checking for new contacts on a POP3 server. You can override this property per mail account. This duration is the interval between the closing of a session and opening a new session with POP3/ IMAP4 email server for the same email account.

5. Click **Ok**.
6. Add the poller server into the poller cluster.

Note:
You must restart the IC Email server on which the poller cluster is mapped.

7. Start the IC Poller Server:

a. On the **Server** tab, select the IC Poller Server.

b. Right-click the IC Poller Server and select **Start**.

For more information about the correct order for starting and stopping IC servers, see Starting and stopping IC servers on page 107.

CAUTION:
Do not start the IC Poller server till it is added to the Poller Cluster or else, the system might crash.

Configuring an IC Email server

The IC Email server interacts with Poller and SMTP servers for polling and forwarding of emails into the IC system from customer to agent. Through workflows, the IC Email server also handles the filtering of spam, the delivery of automatic replies, and the management of traffic flow to external agents and approval agents.

This section includes the following topics:

- Guidelines for an IC Email server on page 329
- Creating the IC Email server on page 329

Guidelines for an IC Email server

Ensure the following:

- A domain should contain only one IC Email server.

Creating the IC Email server

The IC installation program does not automatically add the IC Email server. Email Management requires this server.

To create the IC Email server:

1. In the IC Manager, select **Server** > **New**.
2. From the list of server types, select **Email** and click **Ok**.

3. On the **General** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	Email_<*domain*>	To identify the server, include the domain in the server name.
Domain	IC	For example, select `Email` from the drop-down list if the server is in the Email domain.
Host	IP address of the Email server	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Click the **ICEMail** tab and enter the information in the following fields.

Field	Recommended entry	Notes
IC Data Source	Interaction Center Data Source.	If you used the default name, select `interaction_center`.
Template Admin Port	Accept the default or change if required.	Specifies the port on which the built-in HTTP server listens. If you must change this port, see *Avaya IC Installation Planning and Prerequisites* for a list of the default port numbers used by the other Avaya IC servers. Port conflicts can cause serious problems within the Avaya IC system. If more than one IC Email server is configured on the same host system, ensure that the port number is different for each IC Email server.
Run Analyze Flow	Select this field.	Select this field if you want: • The IC Email server to invoke an email analysis workflow to assist in the routing of incoming email contacts. • To use Analyze with Keywords or Content Analyzer to process incoming email. You must also complete all steps to configure Email workflows to use email analysis. For details, see Using workflows for Email Management on page 348 and the *Avaya IC Media Workflow Reference*.

Field	Recommended entry	Notes
Run Outbound Email Flow	For the initial installation of IC, clear this field.	Select this field if you want to: • Have IC analyze outbound email. • Have a supervisor approve outbound email. • Use Analyze with Keywords or Content Analyzer to process outbound email. You must also complete all steps to configure Email workflows to use email analysis.
AgentPort	Accept the default or change if required.	All IC Agents communicates with the IC Email server on this port. If more than one IC Email server is configured on the same host system, ensure that the port number is different for each IC Email server.

Even if you select the fields in the **ICEmail** tab, the email analysis does not work if you do not perform the steps in the following topics:

- Configuring a Workflow server for Email Management on page 342
- Using workflows for Email Management on page 348
- Creating routing hints for email workflows on page 350

5. Click **Ok**.
6. Add Email server to the IC Email Cluster.
7. Start the IC Email server:
   a. On the **Server** tab, select the IC Email server.
   b. Right-click the IC Email server and select **Start**.

For more information about the correct order for starting and stopping IC servers, see Starting and stopping IC servers on page 107.

CAUTION:
Do not start the IC Email server until it is added to the IC Email Cluster or else, the system might crash.

Configuring Email Template Administration

Email Template Administration requires a Web application. You can configure Email Template Administration on the **Web** tab of the IC Configuration Tool.

This section describes how to install and configure Email Template Administration for each operating system that IC supports. This section includes the following topics:

- Where to configure Email Template Administration on page 333
- Hosting multiple Web applications on a system on page 333
- Advanced properties for Email Template Administration on page 334
- Configuring Email Template Administration on Windows on page 334
- Configuring Email Template Administration on Solaris on page 336
- Configuring Email Template Administration on AIX on page 339

Important:
The Configuration Tool overwrites all manual edits that you make to an IC configuration file.

Where to configure Email Template Administration

Configure Email Template Administration on a system that hosts the templates for Email Management and the Web pages for Email Template Administration.

Hosting multiple Web applications on a system

If the IC system includes more than one Web application on the same system as WebLM, configure all the Web applications on the target system at the same time.

Important:
If you do not configure all of the Web applications simultaneously, keep the options for all Web applications on the target system selected when you re-run the Configuration Tool to create new Web applications. If you keep the options for previously created Web applications unselected, the Configuration Tool may delete those Web applications.

Advanced properties for Email Template Administration

The **Web** tab also includes advanced properties for the Java Virtual Machine.

If you expect a high volume of access to Email Template Administration, you can configure only the advanced properties. For more information, see Configuration Tool advanced properties on page 520.

Configuring Email Template Administration on Windows

If you plan to host Email Template Administration on a Windows system, use the following instructions.

Note:
You do not need to stop the IIS Web server on Windows systems.

To configure Email Template Administration to run on a Windows system:

1. Start the Configuration Tool by selecting **Start** > **Programs** > **Avaya Interaction Center** 7.3 > **Configuration Tool**.

   Note:
   If the Configuration Tool is already open, close and re-open it to ensure that the Configuration Tool includes all system changes, such as new servers.

2. Log in to the Configuration Tool using your IC Manager login ID and password.

3. On the **Web** tab, enter the information for the fields mentioned in the following table:

Field	Description	Sample entry
Tomcat Base Port	The port used to configure the following ports: • Tomcat HTTP ports for Web applications • Tomcat AJP (Web server connector) ports	Default: 9600
IIS Website	The name of the IIS Web server that the Web application will use. **Tip:** For a localized version of IIS, type the localized name for the IIS Web server.	Default website
Web Server Host	The name of the system that hosts the Web server. Do not include the DNS domain.	testbox
DNS Domain	The network (DNS) domain of the system that hosts your Web server. Do not enter an IC domain. **Note:** Verify the default DNS domain and ensure that it is correct.	xyzcorp.com
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: • HTTP port is 80. • HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application for each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: **`http://<server>.<domain>.com:9600/ictest`** **Note:** The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Select the box

4. Select the **Configure Email Template Administration** check box.

Field	Description
Configure Email Template Administration	By default, this field uses the dcobridge1 account that is provided with IC. If you have not already done so, change the default password for this account. **Important:** Do not use the Administrative account for IC Manager or any account for which the password may change.
Email Template Administration Password	Type the password for the account in the IC Login field.

5. Click **Apply Settings**.
6. Click **Ok** on the **Success** dialog box.
7. Click **Exit**.

To ensure that Email Template Administration services started properly

1. Open the Windows Services control panel.
2. Start IC Email Template Management Service 7.3.

   For more information about how to start and stop Web application services, see Starting and stopping IC services on page 114.

Configuring Email Template Administration on Solaris

Use these instructions if you plan to host Email Template Administration on a Solaris system.

Important:
To configure Email Template Administration on Solaris, you must log in as a user with write permissions on the Web server directories and the IC installation directories. The root user usually has these write permissions.

To configure Email Template Administration to run on a Solaris system:

1. Stop the Oracle iPlanet server that hosts the Website application. For information, refer Starting and stopping Oracle iPlanet Web server on page 116.
2. If the Configuration Tool is already open, close it to ensure that the Configuration Tool includes all system changes, such as new servers.

3. Start the Configuration Tool:
   a. Navigate to *IC_INSTALL_DIR*/IC73/bin
   b. Run ./configure
4. Log in to the Configuration Tool using your IC Manager login ID and password.
5. On the **Web** tab, enter the information for the fields mentioned in the following table:

Field	Description	Sample entry
Tomcat Base Port	The port used to configure the following ports: • Tomcat HTTP ports for Web applications • Tomcat AJP (Web server connector) ports	Default: 9600
Web Server Home	The installation path for the Oracle iPlanet Server that hosts the Web application.	/opt/oracle/webserver7
Web Server Name	The root name of the server as found in the Oracle iPlanet Server home directory. **Note:** Do not include https- in the Web server name.	testbox.xyzcorp.com
Web Server Host	The name of the system that hosts the Web server. Do not include the DNS domain.	testbox
DNS Domain	The network (DNS) domain of the system that hosts your Web server. Do not enter an IC domain. **Note:** Ensure that the default DNS domain is correct.	xyzcorp.com

Field	Description	Sample entry
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: • HTTP port is 80. • HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application on each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: **`http://<server>.<domain>.com:9600/ictest`** **Note:** The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Select the check box

6. Select the **Configure Email Template Administration** check box.

Field	Description
Configure Email Template Administration	By default, this field uses the dcobridge1 account that is provided with IC. If you have not already done so, change the default password for this account. **Important:** Do not use the Administrative account for IC Manager or any account for which the password may change.
Email Template Administration Password	Type the password for the account in the IC Login field.

7. Click **Apply Settings**.
8. Click **Ok** on the **Success** dialog box.
9. Click **Exit**.

To ensure that Email Template Administration services started properly:

1. In the Oracle iPlanet Server installation directory:
   a. Open the admin-server directory.
   b. If the directory includes a file called start-ICEnv.backup, execute the following command to rename the file:

      ```
      mv start-ICEnv.backup oldstart-ICEnv
      ```
2. Start the Oracle iPlanet server that hosts the Website application. For more information, see Starting and stopping Oracle iPlanet Web server on page 116.
3. Navigate to the *IC_INSTALL_DIR*/IC73/bin directory.
4. Use the following script to start Tomcat

   ```
   nohup ./ictomcat.sh start rlmanager
   ```

Important:
For Solaris only, the Configuration Tool changes the ownership of the implementation file (vesp.imp) and the interface file (vespidl.pk) to root. If you do not want to run IC as root, you must change the ownership of these files as described in Changing the ownership for IC on page 49.

Configuring Email Template Administration on AIX

Use these instructions if you plan to host Email Template Administration on an AIX system.

Important:
To configure Email Template Administration on AIX, you must log in as a user with write permissions on the Web server directories and the IC installation directories. The root user usually has these write permissions.

To configure Email Template Administration to run on an AIX system

1. Stop the IBM HTTP Server that hosts the Website application with the stop script packaged with the Web server: **`./httpserver.sh stop`**
2. Start the Configuration Tool:
   a. Navigate to *IC_INSTALL_DIR*/IC73/bin
   b. Run `./configure`

   If the Configuration Tool is already open, close and re-open it to ensure that the Configuration Tool includes all system changes, such as new servers.
3. Log in to the Configuration Tool using your IC Manager login ID and password.

4. On the **Web** tab, enter the information for the fields mentioned in the following table:

Field	Description	Sample entry
Tomcat Base Port	The port used to configure the following ports: • Tomcat HTTP ports for Web applications • Tomcat AJP (Web server connector) ports	Default: 9600
Web Server Home	The installation path for the IBM HTTP server instance that hosts the Web application.	`/usr/HTTPServer`
Web Server Host	The name of the system that hosts the Web server. Do not include the DNS domain.	testbox
DNS Domain	The network (DNS) domain of the system that hosts your Web server. Do not enter an IC domain. **Note:** Verify the default DNS domain carefully to ensure that it is correct.	xyzcorp.com
Web Server Port	The port that your Web server uses for communication. Make sure that the port matches the protocol used by your Web server for communication. The default ports are: • HTTP port is 80. • HTTPS port is 443. Do not change the default port unless you assign a different port to the Web server.	Default: 80
IC Test	Optional. IC Test is a Web application that you can use to test your Tomcat configuration. If you install multiple versions of Tomcat, the Configuration Tool creates an IC Test application on each version of Tomcat. The Configuration Tool also creates a separate Tomcat server to host IC Test. To access IC Test, use the Tomcat HTTP port in the URL. For example, type: **`http://<server>.<domain>.com:9600/ictest`** **Note:** The port number is not required if you install a single version of Tomcat, or access IC Test from the separate Tomcat server for IC Test.	Select the check box

Comments on this document? infodev@avaya.com

5. Select the **Configure Email Template Administration** check box.

Field	Description
Configure Email Template Administration	By default, this field uses the dcobridge1 account that is provided with IC. If you have not already done so, change the default password for this account. **Important:** Do not use the Administrative account for IC Manager or any account for which the password may change.
Email Template Administration Password	Type the password for the account in the IC Login field.

6. Click **Apply Settings**.
7. Click **OK** on the **Success** dialog box.
8. Click **Exit**.

To ensure that Email Template Administration services started properly

1. Start the IBM HTTP Server that hosts the Website application, as described in Starting and stopping IBM http Web server on page 119.
2. Navigate to the *IC_INSTALL_DIR*/IC73/bin directory.
3. Use the following script to start Tomcat:

   ```
   nohup ./ictomcat.sh start rlmanager
   ```

   Important:
   For AIX only, the Configuration Tool changes the ownership of the implementation file (vesp.imp) and the interface file (vespidl.pk) to root. If you do not want to run IC as root, you must change the ownership of these files as described in Changing the ownership for IC on page 49.

Setting the options in Internet Explorer

If you are using RLManager on a system that uses Microsoft Internet Explorer 10 and Internet Explorer 11, then you must disable compatibility mode before running RLManager template administration.

Configuring a Workflow server for Email Management

To configure the Workflow server for Email Management, perform the steps in the following topics:

1. Creating a Workflow server for Email Management on page 342.
2. Creating email channels for the Workflow server on page 343.
3. Starting the Workflow server on page 348.

If your IC system includes multiple Workflow servers, perform these steps on each Workflow server that handles pre-qualification for email contacts and routes email contacts.

Creating a Workflow server for Email Management

These instructions only provide information about those parameters you need to set when you create a Workflow server to handle email contacts. For more information about other parameters in the Workflow server, see Configuring multiple Workflow servers on page 94 and *Interaction Center Administration Guide*.

CAUTION:
If you do not configure the Workflow server with synchronous startup flows, the Qualify Email workflow cannot resolve the pkey of the queue where a contact is to be routed. If this occurs, IC cannot route email contacts.

To create a Workflow server for Email Management

1. In IC Manager, select **Server** > **New**.
2. From the list of server types, select **Workflow**.
3. Click **OK**.
4. On the **General** tab, and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	Workflow_<*domain*>	Include the domain in the server name to identify the server.

Field	Recommended entry	Notes
Domain	Select the IC domain for the server from the drop-down list.	For example, select `Email` to use the pre-configured domain for Email Management.
Host	Select the IP address of the system from the drop-down list, or type the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

5. Click the **Workflow** tab.
6. From the **IC Data Source** drop-down list, select the Interaction Center data source.

   The default name for this data source is `interaction_center`. This is the data source that you created in Generating the Interaction Center application on page 151.
7. Select **Synchronous Startup Flows.**
8. If the following rows do not exist, add them to the Synchronous Startup Flows:
   a. Click **New**.
   b. In the new row, type `web_routing.update_qw_cache`
   c. Click **Ok**.
9. Continue creating email channels for workflow servers as mentioned in Creating email channels for the Workflow server on page 343.

Creating email channels for the Workflow server

You must add email channels and associations with the workflows for each channel. You create separate channels for email qualification and for email analysis. Use different Workflow servers to handle each task and create these channels in the appropriate Workflow.

Important:
In case you have configured two WebACD servers then deploy 2 Email Management Workflow servers in those domains. For example, if `Web` and `Web2` are two domains where you have configured `WebACD1` server and `WebACD2` server respectively, you must configure Email Management Workflow servers in both `Web` and `Web2` domain.

This section includes the following topics:

- Creating the email channel for email qualification on page 344.
- Creating the email channel for email analysis on page 345.

Creating the email channel for email qualification

Perform these steps in each Workflow server that runs the Qualify Email workflow.

To create an email channel for a Workflow server that qualifies emails:

1. In the Server Editor for the Workflow server, click the **Channels** tab.
2. Click **New Channel** on the toolbar.
3. In the **Channel Editor** dialog box, enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Global	Do not select this field.	Do not select this field to create a channel for a specific server or media, such as Email.
By Server	• Do not select this field if you want the channel to handle events from all servers of the type that you select from the **Service** drop-down list. • Select this field if you want the channel to handle events only from a specific server that you select from the **Service** drop-down list.	If you select this field, and you need this Workflow server to communicate with more than one server, you must create another channel for that server. **Warning:** If you select this field and the WebACD server is named "WACD", the Workflow server cannot communicate with the WebACD server.
Channel Range	No entry necessary.	Completed by IC Manager
Service	Select **WACD** or the WebACD server from the drop-down list.	Whether you can select a server or a type of server, depends up whether or not you have selected the **By Server** field.
Criteria	Type **media=email**	The field value is case sensitive. You must specify the value as mentioned.

4. Click **Ok** in the **Channel Editor** dialog box.
5. Select the channel that you created in the step above.
6. Click the **New Association** button on the toolbar.

7. In the **Channel Association** dialog box, enter the information for the fields mentioned in the following table:

Field	Recommended entry
Channel Range	Completed by IC Manager
Service Interface	Completed by IC Manager
Event	WACD.QualifyEmail **Note:** This field value is case-sensitive and must follow the format **<*flow_project*>.<*flow_name*>**
Flow	**<*flow_project*>.<*flow_name*>** For example, type **wacd.qualifyemail** **Note:** This field value is case-sensitive and must follow the format **<*flow_project*>.<*flow_name*>**

8. Click **Ok** in the **Channel Association** dialog box.
9. Perform one of the following steps:
   - Click **Ok** in the Server Editor to complete the Workflow server configuration.
   - If the Workflow server also runs email analysis workflows, continue with Creating the email channel for email analysis on page 345.

Creating the email channel for email analysis

Perform these steps in each Workflow server that will run the email analysis workflow.

To create an email channel for a Workflow server that analyzes emails:

1. In the Server Editor for the Workflow server, click the **Channels** tab.
2. Click the **New Channel** button on the toolbar.

3. In the **Channel Editor** dialog box, enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Global	Do not select this field.	Do not select this field to create a create a channel for a specific server or media, such as Email.
By Server	• Do not select this field if you want this channel to handle events from all servers of the type that you select from the **Service** drop-down list. • Select this field if you want this channel to handle events from only one specific server that you select from the **Service** drop-down list.	If you select this field, and you need this Workflow server to communicate with more than one server, you must create another channel for that server. **Warning:** If you select this field and the WebACD server is named "WACD", the Workflow server will not be able to communicate with the WebACD server.
Channel Range	No entry necessary.	Completed by IC Manager
Service	Select **ICEMail** from the drop-down list.	Whether you can select a server or a type of server, depends up whether or not you checked the **By Server** field.
Criteria	Type *****.	

4. Click **Ok** in the **Channel Editor** dialog box.
5. Select the channel that you created in the step above.
6. Click the **New Association** button on the toolbar.

7. In the **Channel Association** dialog box, enter the information for the fields mentioned in the following table to create an inbound and an outbound association for the email channel.

Channel or Association	Field	Recommended entry
Association 1	Channel Range	Completed by IC Manager
	Service Interface	Completed by IC Manager
	Event	ICEmail.Analyze **Note:** This field is case-sensitive and must follow the format ***<flow_project>.<flow_name>***
	Flow	***<flow_project>.<flow_name>*** For example, enter one of the following: • **icemail.analyzenoca** if your system does not include Content Analyzer • **icemail.analyzeca** if your system includes Content Analyzer
Association 2	Channel Range	Completed by IC Manager
	Service Interface	Completed by IC Manager
	Event	ICEmail.OutboundEmail **Note:** This field is case-sensitive and must follow the format <***flow_project***>.<***flow_name***>
	Flow	<***flow_project***>.<***flow_name***> **Note:** This field value is case-sensitive and must follow the format: <***flow_project***>.<***flow_name***> For example, enter one of the following: • **icemail.outboundnoca** if your system does not include Content Analyzer • **icemail.outboundca** if your system includes Content Analyzer

8. Click **Ok** in the **Channel Association** dialog box.
9. Click **Ok** in the Server Editor to complete the Workflow server configuration.

Starting the Workflow server

To start the Workflow server:

1. In IC Manager, right-click the Workflow server that handles email contacts and select **Start**.

Using workflows for Email Management

You can use the sample workflows to configure and test your Email Management servers. IC seed data includes compiled sample workflows. When you import seed data into the CCQ database, you are storing the compiled workflows in the database.

Note:

ICEmail flows, such as **analyzenoca**, **analyzeca**, **outboundca**, and **outboundnoca** are not seeded for fresh IC 7.3 install. Therefore, you must manually build these flows in Workflow Designer and upload these flows to the database.

Email Management uses the following sample workflows:

- An incoming and outbound Email Analysis workflows from the ICEmail project
- The Qualify Email workflow in the WACD project
- All Web Management workflows, see Using workflows for Web Management on page 232

Before your IC system moves into production, you can modify the properties of the sample workflows to meet the requirements of your contact center. For example, you can route an outbound email to an approval queue or to an approving agent. For more information, see *Avaya IC Media Workflow Reference*.

Configuring Outbound Email Analysis workflows

The ICEmail project contains two sample Outbound Email Analysis flows. The sample Outbound with Keywords workflow (outboundnoca) performs analysis on outbound email in IC systems that do not include Content Analyzer. The sample Outbound with Content Analyzer workflow (outboundca) performs analysis on outbound email in IC systems with Content Analyzer.

The sample Outbound Email Analysis flows depend on settings in the following:

- Outbound settings in the IC Email server
- Email channel in the Workflow server

- Group properties in IC Manager
- Blocks in the Qualify Email workflow
- Blocks in the Outbound Email Analysis workflow

You must know the configuration of your production environment before you can configure the Outbound Email Analysis flows to work in your IC system. Therefore, until you have tested your Email Management system and know the configuration of your production environment, you should not run any Outbound Email Analysis flows. For more information on this setting, see Creating the IC Email server on page 329.

If you want to run an Outbound Email Analysis workflow in your Email Management system, you must configure and test your system carefully.

To configure Outbound Email Analysis:

1. In Workflow Designer, open the appropriate Outbound Email Analysis workflow in the ICEmail project, as shown in the following table:

Workflow	IC system configuration
outboundca	IC systems with Content Analyzer.
outboundnoca	IC systems without Content Analyzer.

2. Double-click the GetAgentQuota block and in the Property Sheet:
   a. Click the **Basic** tab.
   b. Set the value of **`DefaultQuotaValue`** to 0 (zero).

      If you set the default value to 0 (zero), outbound email contacts are not reviewed.
3. Save and recompile the workflow.
4. In IC Manager, set the group properties for agents
   a. Select **Tools** > **Groups** > **Properties** to open the **Group Properties** dialog box:
   b. Select Email/Agent and set the value of the ReviewQuota property.

      If you set the default value to 0 (zero), outbound email contacts are not reviewed.
   c. Apply and save the changes.

   For more detailed instructions, see Setting global properties for all agents on page 385.
5. In IC Manager, if you configured any agents not to cascade their properties from the global properties, set the value of ReviewQuota to 0 (zero) for those agents also. For more detailed instructions, see Setting properties for individual agents and workgroups on page 385.

Creating routing hints for email workflows

The sample email workflows contain blocks that use routing hints from the RoutingHint table in the Directory server to analyze and route email contacts. These blocks include:

- Fetch Routing Hints (email) block in the Qualify Email workflow
- Set Routing Hint blocks in each of the Email Analysis workflows

Important:
Routing hints must be in lower case. Do not use mixed upper and lower case in your routing hints. If the routing hint is not in all lower case, the workflow cannot locate the routing hint, and Avaya IC cannot correctly route the contact.

For more information about the sample email workflows and how the workflows use routing hints, see *Avaya IC Media Workflow Reference*.

The email workflows use hints from the RoutingHint table to route email contacts.

Each row in the routing hint table contains the following:

- A routing hint
- The IDs of the queues where contacts that match the routing hint should be routed

Tip:
The default email queue is **DefaultEmailQueue@DefaultTenant**. You can create and use additional email queues for routing email contacts. For more information, see *Interaction Center Administration Guide*.

The routing hints that you need to create for the sample email workflows depend upon your IC system. The following table describes the routing hints required by the different sample email workflows.

IC deployment	Email workflow	Routing hints
Email contact routing	wacd.qualifyemail	If deployment includes email analysis, no additional hints required. If no email analysis, create a routing hint for the To address of email. For example, incomingemail@ic.avaya.com

IC deployment	Email workflow	Routing hints
Email Analysis with Keywords	icemail.analyzenoca	Create a routing hint with a value such as: • sales • support • printers
	icemail.outboundnoca	Create a routing hint with a value of: • approvalrequired
Email Analysis with Content Analyzer	icemail.analyzeca	Create a routing hint with a value such as: • home computing • desktop Also, create routing hints for language with an ISO-639-1 value such as: • en • sp • fr • de • zh
	icemail.outboundca	Create a routing hint with a value of: • approvalrequired • suspectcontent

To create routing hints

1. In IC Manager, click the **Configuration** tab.
2. In the left pane, select **Tables** > **Workflow** > **RoutingHint**.
3. Click the **New** button on the toolbar.

4. In the right pane, enter the information for the fields mentioned in the following table:

Parameter	Recommended entry	Description
Routing Hint	Type a routing hint.	Type the name of a routing hint required by a sample email workflow. The routing hint must be a single word in all lower case, and cannot contain any special characters.
Email Queue ID	Type `DefaultEmailQueue@DefaultTenant`.	DefaultEmailQueue@DefaultTenant is the default email queue. For more information about email queues, see *Interaction Center Administration Guide*.
Category/ Qualifier	Leave this field blank.	
Tenant	Select `DefaultTenant` from the queue from the drop-down list.	Select the tenant used by the queue. For the DefaultEmailQueue, select DefaultTenant to ensure that the routing hint uses the correct queue.

5. Click **Ok**.
6. Click **Apply**.

   Repeat Steps 3 through 6 to create all required routing hints.
7. Select **Manager** > **Refresh**.

Configuring the WebACD server for Email Management

Configuration of the default email cluster is required for agents to communicate to IC Email server.

Important:
Ensure that the email servers in the default email cluster are always running.

To configure the default email cluster in the WebACD server

1. In IC Manager, double-click the **WACD** server in the lists of server types.
2. Click the **WACD** tab.

3. In the **Default Email Cluster**, drop-down list, select the email cluster that you want to use for configuring WebACD.

   Note:
   You must configure the email cluster before you configure the WebACD server for email management.

4. Click **Ok**.

   Note:
   In case of two WebACD servers, you must configure the default email cluster on both the WebACD servers.

Integrating Email Template Administration

Perform these steps to launch the Email Template Administration Tool from IC Manager.

Tip:
You need to complete only those properties listed in this section to integrate Email Management administration.

To configure Email Template Administration:

1. In IC Manager, select **Tools** > **Groups**.
2. Click the **Properties** tab.
3. In the left pane, select **IC**.
4. In the **Sections** list, select **System/Configuration**.
5. Select the following properties:
   a. Click **Edit**.

b. Set values for the properties, as shown in the following table:

Property	Recommended entry
EmailLoginServer	Type the fully-qualified domain name of the server that hosts the Email Template Administration pages. For example, type **ICEmail.xyzcorp.com**.
EmailLoginServerPort	Type one of the following ports for the IC Email server web port: • HTTP - 80 • HTTPS - 443 Do not change the default port.
EmailLoginServerWebsite	Type **rlmanager** as the name of the Response Library Manager web application. The Configuration Tool defined this application name when you configured Email Template Administration.
EmailServer	Type the fully-qualified domain name of the system that hosts the IC Email server.
EmailServerPort	Type the IC Email server HTTP port. For example, the default is 19114.

If one of these properties is not available, select **Property Insert** and select the property name from the drop-down menu.

Tip:
If the columns in the right pane are Name, Entity, Value, and Overridable, select the **- (minus)** button on the toolbar to view and edit these properties.

6. Click **Apply**.
7. Click **Ok**.

Configuring email accounts

You must configure Email Management to use your mail accounts to:

- Retrieve inbound email from customers
- Send outbound agent replies

The following table describes the email accounts that must exist before you configure Email Management to use email accounts.

Required email accounts	Description
Email Management mail accounts	These accounts must exist as mailboxes on the POP3 or IMAP4 server or on Exchange Online. Note the login ID and password. IC Manager can only link to an existing mailbox. IC Manager cannot create mailboxes on a POP3 or IMAP4 server or on Exchange Online.
At least one email account for the Customer account for inbound customer messages	Web Management uses customer email accounts to send email from the customer website to your contact center. Use this email address for mailto: links on your website and wherever you plan to make email addresses available to customers.
Bounced email account	Email Management uses this account as the destination address for emails sent by the IC Email server that the SMTP server bounces or rejects. All filtered spam and other junk emails also get forwarded to this bounced email. You include this account in your IC Email server configuration.
Disabled accounts (optional)	You can set up Disabled accounts to test or troubleshoot the following servers: • Web Management servers • IC Email server • Tomcat server where you install the website application Email Management does not retrieve messages for disabled accounts.

Email Management can manage mailboxes in any number of domains as long as it has the necessary information to log onto the POP3 or IMAP4 server or onto Exchange Online.

Tip:
The IC Poller Server generates the "to address" for an incoming email from the **Name** and **Domain** fields on the **General** tab of the **Email Account Configuration** window. As a result, the logon account does not need to match the first part of the email address, and the "to address" is independent of the logon account used to poll the POP3 or IMAP4 server.

To add a POP3/IMAP4 email account to Email Management:

1. In IC Manager, select **Services** > **Email Accounts**.
2. In the **Email Accounts** dialog box, click **New**.

3. In the **New Email Account** property sheet, enter the information for the fields mentioned in the following table.

Tab	Field	Description
General tab	Display Name	The name that the email client application displays for the configured email address. For example, if support@testdomain.com is an actual email address and Support Test is the display name for the email address, the email client application at the customer end shows the display name in the From address of the email that they receive from agents.
	Name	Type the mailbox name exactly as it is configured in your POP3 or IMAP4 server or Exchange Online. Forexample, type **agent**.
	Domain	Type the mailbox domain exactly as it is configured in your POP3 or IMAP4 server or Exchange Online. Forexample, type **xyzcorp.com**.
	Tenant	Select the tenant from the drop-down list to associate with this email account.
	Return address	Select the address that appears in the **From** field in an email response sent to the customer from this account. By default, IC Manager automatically completes this field with **name@domain**.
	Bounce Email Address	Type the email address to which the bounced email are sent.
	Owner Name	Select the poller cluster for which the email account is configured.
	Disable Account	Select the check box to temporarily disable the email account.
Outgoing Email Server tab	Email Account Type	Outgoing protocol. SMTP or Graph.
	Outgoing Email Server (SMTP)	Type the network address for the SMTP email server you would like to use here.
	Outgoing Email Server (SMTP) Port	Type the port number for the SMTP server. The default port is 25.

Tab	Field	Description
	Use TLS	The options are: • None: This means that TLS is not used. • TLS: Selecting this value will ensure that TLS is used. When you select TLS, the default Outgoing Email Server (SMTP) Port changes to 465. • STARTTLS: Selecting this value will ensure that STARTTLS is used. **Note:** If you select STARTTLS or TLS option then you must install the SMTP CA certificate in the Avaya core server on which ICEmail server is running. The certificate must be in PEM format with the filename as the <Outgoing Email Server(SMTP)>.pem. For Website and ICM to send outbound email using SSL SMTP you must import the SMTP CA certificate in the Java Keystore where Website and ICM are configured. For more details see Importing the CA certificate in the JAVA Keystore on server machine where Website and ICM are configured for SSL SMTP on page 312.

Tab	Field	Description
	Use SMTP Authentication	Select this option to enable SMTP AUTH. If this option is selected, you can view the following options: • Logon account: Provide the login detail for SMTP AUTH. • Password: Provide the password for SMTP AUTH. (is not required when the XOAUTH2 authentication type is used). • Confirm Password: Re-enter the password. (is not required when the XOAUTH2 authentication type is used). • Use Secure Authentication: Select this option to send SMTP AUTH info securely. • Authentication Type: This option is enabled if you select Use Secure Authentication option. The available options under Authentication Type are: – LOGIN – NTLM – CRAMMD5 – XOAUTH2
	Logon account	Provide the login detail for Graph.

Tab	Field	Description
	Test	Click this button to test the email account for the outgoing mail server. If you want to send a sample email as well as test the connection, select the **Send a test message using this account** check box. IC Manager creates an email with: • A dummy address in the **From** field • The selected email account in the **To** field • The current timestamp in the **Subject** field. • The phrase "Test mail message" in the **Body** field. If you want to change any of the default information, you can change the value in the appropriate field. **Note:** If you select **Use SMTP Authentication** option then the **Test** button is disabled. • Click **Test**, to send that email to the SMTP server. You can use this option to generate multiple test emails and compare the timestamp in their subject lines.
Incoming Email Server tab	Email Account Type	Select **POP3** or **IMAP4** or **GRAPH** from the drop-down list. In IC 7.3, you can also use IMAP4 protocolfor receiving the emails. In IMAP4, all the mailsremains on the mail server. If you select IMAP4, the **Mail Folder Name** field becomes visible. In this field, you have to enter the exact name of the folder from which you want fetch the emails. For example: • To access the nested folder `support_requests`, which is inside the `INBOX/Support` folder, you must enter `INBOX/Support/support_requests`. • To access the root folder `INBOX` or `New Requests`, you must enter `INBOX` or `New Requests`.

Tab	Field	Description
	Incoming Email Server	Type the network address of the POP3 or IMAP4 server where the email accounts are configured, the logon account, and password in the appropriate field. **Note:** If any of these settings are incorrect, Email Management will not be able to connect to the POP3 or IMAP4 email server. **Note:** For email accounts with TLS enabled, the incoming server name should be Fully Qualified Domain Name (FQDN). For example, `hostname.domainname`.
	Incoming Email Server Port	Type the port number for receiving mails from POP3 and IMAP4 server. By default, the port number for POP3 sever is 110 (995 if TLS is enabled) and IMAP4 server is 143 (993 if TLS is enabled).
	Logon account	Enter the name of the email account. You do not need to enter the domain.
	Password / Confirm	Enter the password for the email account in both of these fields. (is not required when the XOAUTH2 authentication type is used).
	Use TLS	Select this field to enable the TLS (Transport Layer Security) for the mails that are fetched from this email account. For more information, see Configuring the email accounts for SSL on page 363. If you select this option, the IMAP4/ POP3 works on the SSL port, which is 993/ 995.
	Use Secure Authentication	Select this check box to secure the username and password over the network. Secure Password Authentication is a challenge-response protocol used by the Windows security subsystem to prevent passwords from being sent through the network in plain text. Your POP3 or IMAP4 server must support Secure Password Authentication to use this option.
	Authentication Type	Select **NTLM, MD5** or **XOAUTH2** as authentication types for this email account. For more information, see Configuring the email accounts for SSL onpage 363.
	Test	Click the button to test the email account for incoming mail server.

Tab	Field	Description
OAuth tab	Client ID	Enter Client ID of the registered Azure application.
	Authority	Enter common part of an authority url in form https://login.microsoftonline.com/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx.
	Secret	Enter client secret. Usable only in Graph mode.
	Redirect URI	Enter Redirect URI of application. Must be http://localhost.
	Scopes	Enter scopes for the registered Azure application divided by semicolon. Typical value for OAuth2 is *offline_access; https://outlook.office.com/IMAP.AccessAsUser.All; https://outlook.office.com/POP.AccessAsUser.All;* *https://outlook.office.com/SMTP.Send* and for Graph *offline_access;https://graph.microsoft.com/.default* **Note:** We recommend that you set up Exchange Online and everything related to it by contacting its administrator.

Comments on this document? infodev@avaya.com

Templates tab	-	The **Templates** tab allows you to specify the following templates: • **Header:** The template specifies the text to be inserted at the top of any email that you are sending to a customer. • **Footer:** The template specifies the text to be appended to the end of any email that you are sending to a customer. • **New Message:** The template specifies the text to be automatically sent to a customer when a new email is received from the customer. • **Follow Up:** The template specifies the basic acknowledgement message to be sent when a customer replies to a message sent from IC or a follow up email is received from the customer. • **Bounce Mail:** The template specifies the text that will be sent automatically in response to message that has been rejected. You can create these templates in **Email Template Administration**. For more information, see Configuring Email Template Administration on page 333
Filter tab	Filter Type	Select the type of filter to be enabled for this email account. **Note:** At a time, only one filter is active.
	Accept From	Click the button to enter email addresses. Email management rejects mails that comes from an email address that is not in the **Accept From** list. The field is enabled only if you select the filter type as **VALID_EMAIL_LIST**.
	Reject From	Click the button to enter email addresses. Email management rejects mails that comes from any email address mentioned in the **Reject From** list. The field is enabled only if you select the filter type as **INVALID_EMAIL_LIST**.

Tab	Field	Description
Miscellaneous tab	Override global email checking scheduler	Select this box if you want this account to check for new messages either more or less frequently than the global setting that was specified for the IC Poller Server.
	New email check frequency (sec)	Specifies the number of seconds that the email server waits for checking new contacts on a POP3 or IMAP4 server. This duration is an interval between closing of a session and opening a new session with POP3/IMAP4 email server for same email account. You must check **Override global email checking scheduler** to use this field.
	Duplicate Message Checking	Select the check box to enable the checking of duplicate message received by an agent. Selecting this options ensures that duplicate messages are not received. The option does not check outbound email contacts. An incoming email contact is considered to be a duplicate if all of the following parts of the contact are identical to those in a previous contact: • From address • To address • Subject • Body
	Loop Detection	Select the check box to enable the loop detection.
	Loop Detection Type	Loop detection is based on "sender", "from address", "reply to address" or "both".
	Loop Detection Template	Click the button to select the template for the loop detection type selected above.
	Blank Template Detection	Select this check box to set the Blank Email template.

Tab	Field	Description
	Blank Email	The templates specifies the text that are automatically sent to a customer when a blank email (for example, an email with no body text) is received from a customer. You must select the **Blank Template Detection** check box.
	Loop Detection Count	The maximum number of automated responses that you want the customer to receive in a 24-hour period. **Note:** Email Management does not automatically respond to messages that exceed this count.

4. Click **Ok**.

For more information about how to create IC email accounts, see *Interaction Center Administration Guide*.

Configuring the email accounts for SSL

Currently IC allows you to configure all the POP3 email accounts either with Windows NT Lan Manager (NTLM) or Message-Digest algorithm 5 (MD5) security authentication types. These authentication methods allow only the password to be secured over the network. From IC 7.3 release, you can configure all your POP3 and IMAP4 email accounts with the SSL security.

To enable SSL for email accounts you require:

- **Server Certificate:** This needs to be generated using a certificate request to certificate authority for the exchange server and will be added to the exchange server.
- **CA chain Certificates:** This consist of the Root certificate, the signing CA certificate, and all the relevant intermediary CA signing certificates, in a single file in `.PEM` format.The 'CA chain' file should be placed in `Avaya/IC73/etc` directory, on the machine where the Poller and ICEmail servers reside.

The SSL security in IC requires that you configure a Server side certificate on the exchange server and CA chain certificates on the systems hosting the Poller and ICEmail servers.

The CA Chain certificates must be in the `.PEM` format, and the certificate file name is in the `host name.domain name` format. The `host name` is the name of the system where the exchange mail server is configured, and the `domain name` is the name of the domain in which the exchange mail server resides. This should be the same as the `hostname.domain` configured for that email account in IC Manager.

The CA chain certificates with a different format must be converted to `.PEM` format.

Important:
Do not change the certificate format by manually changing the extension. You must use the `OpenSSL` utility for converting the format of the certificate.

Note:
Before configuring an email account with the SSL security, ensure that your mail servers are configured with the required server certificates received from a certified authority, such as VeriSign or Thawte.

You can enable the SSL security for any email account by selecting an option in the email account configuration. For more information, see the table in the Configuring email accounts on page 354.

Creating certificate request for POP3 or IMAP4 server for SSL

In IC, selecting the TLS option to enable the SSL security requires a certificate to be created and installed on the exchange server. This section explains the procedure to create a certificate for POP3 or IMAP4

To create certificate for POP3 or IMAP4

1. From the Windows **Start** menu, select **Programs** > **Microsoft Exchange** > **System Manager**.
2. In the left pane, expand the **Servers** node.
3. Select a mail exchange server.
4. For the selected server, select **Protocols** > **POP3**.
5. Right-click the **Default** option and select **Properties**.
6. On the **Default POP3 Virtual Server Properties** window, click the **Access** tab.
7. In the **Secure Communication** section, click **Certificate**.
8. By keeping the default options selected click **Next** on the following pages:
    1. Server Certificate
    2. Delayed or Immediate Request
    3. Name and Security Settings
9. Click **Next**.
10. On the **Your Site's Common Name** page, enter the complete server name including the domain as common name. For example, `puicdev111.pop.ic.com`.

    Note:
    The common name you entered here is used for naming the Root Certificate.
11. Click **Next**.
12. Click **Next**.

13. Enter the certificate file name and click **Next**.

Note:
Follow the same procedure for creating certificate request for IMAP4.

Creating Certificates using Microsoft CA

After you create a request for creating certificate, you need to create a certificate and get it downloaded on the server. This section explains the procedure for doing this.

To create a certificate

1. On the exchange server, open the Internet Explorer.
2. In the address bar, type: **`http://localhost/certsrv`**.
3. Click the **Request a certificate** link.
4. Click the **advanced certificate request** link.
5. Click the **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file** link.
6. On the **Submit a Certificate Request or Renewal Request** page, paste the contents of the certificate text file that you have created while creating certificate request. For more information, see Creating certificate request for POP3 or IMAP4 server for SSL on page 364.
7. In the **Certificate Template** drop-down list, select **Web Server** as the certificate template.
8. Click **Submit**.
9. On the **Certificate Issued** page, select **Base 64 encoded** option.
10. Click the **Download certificate** link.
11. Save the certificate.

    The certificate is in the `.CER` format. You need to convert this certificate in the `.PEM` format. For more information, see Converting root certificate from .CER format to .PEM format on page 367.

Note:
For Certificate Authority other than Microsoft CA, you must send the request to the respective Certificate Authority.

Adding Certificate to POP3 or IMAP4 Server

After you create and download the certificate, you need to add the certificate to a proper location on the POP3 or IMAP4 server. This section explains the procedure for doing this.

To add certificate to POP3 or IMAP4 server

1. From the Windows **Start** menu, select **Programs** > **Microsoft Exchange** > **System Manager**.

2. In the left pane, expand the **Servers** node.
3. Select a mail exchange server.
4. For the selected server, select **Protocols** > **POP3**.
5. Right-click the **Default** option and select **Properties**.
6. On the **Default POP3 Virtual Server Properties** window, click the **Access** tab.
7. In the **Secure Communication** section, click **Certificate**.
8. On the **Pending Certificate Request** page, click **Next**.
9. Select the certificate file converted into the `.PEM` format.
10. Click **Next** to add a certificate.

Activating TLS settings on POP3 or IMAP4 server

To activate TLS to POP3 or IMAP4 server

1. From the Windows **Start** menu, select **Programs** > **Microsoft Exchange** > **System Manager**.
2. In the left pane, expand the **Servers** node.
3. Select a mail exchange server.
4. For the selected server, select **Protocols** > **POP3**.
5. Right-click the **Default** option and select **Properties**.
6. On the **Default POP3 Virtual Server Properties** window, click the **Access** tab.
7. In the **Secure Communication** section, click **Communication**.
8. On the Security dialog box, select **Require secure channel** and **Require 128-bit encryption**.
9. Click **OK**.

Downloading Root Certificate from the Microsoft CA

To download a root certificate

1. On a local system, open the Internet Explorer.
2. In the address bar, type: **`http://localhost/certsrv/`**.
3. In **Encoding method**, select **Base 64**.
4. Click the **Download CA Certificate** link.

Note:

The certificate is in the `.CER` format. Change the `.CER` file name to your site's Common Name, which was used while Creating certificate request for POP3 or IMAP4 server for SSL on page 364. For Certificate Authority other than Microsoft CA, you must obtain the Root Certificate from respective Certificate Authority.

You need to convert this certificate in the `.PEM` format. For more information, see Converting root certificate from .CER format to .PEM format on page 367.

Important:

After you convert the certificate to `.PEM` format, you must copy the Root certificate to the *`IC_INSTALL_DIR`*`\IC73\etc` directory of the local system where Poller server is running.

Converting root certificate from .CER format to .PEM format

You must convert the Root certificate to `.PEM` format

To convert certificate format:

1. Run the Command Prompt.
2. Type the following command:

   `openssl x509 -in <certificatename.cer> -out <certificatenewname.pem> -outform PEM`

   The `certificatenewname` must be in the form: `host name.domain name`.

Creating an email status

An agent can select an email status from a scrollable list in Avaya Web Agent. The agent selects a status to resolve an email contact. You can use Mail Template Administration from IC Manager to create the different types of email status that appear in the list.

For more information on how to create an email status, see *Interaction Center Administration Guide*.

To create an email status:

1. In IC Manager, select **Services** > **Mail Template Administration**.

   If prompted, log in to Email Template Administration with the same login ID and password that you used for IC Manager.

2. Click **New**.
3. Select **New Status**.

4. In the **New Status Properties** dialog box, complete the following fields:
   a. Type a name for the status in the **Name** field.

      This text is displayed on the list of statuses available to agents in Avaya Agent.

   b. Select the check boxes shown in the following table, if required:

Check box	Recommended entry
Messages set to this status should be treated as answered	Select this box if the status indicates a resolution of the issue that requires no further action by the agent.
Send template for this status	Select this box if you want to send an auto-response message to the user when an agent assigns this status to a message. Choose a template to send. If you do not know the location of the template, select **Browse** and navigate to the required template. **Note:** Auto-response is sent when an email contact is processed by the ICEmail server after the Poller server delivers the contact to the ICEmail server. Therefore, at times, when there is considerable email load, auto-responses might not be sent immediately after the email is polled by the Poller server. However, auto-responses might be sent after some delay when the ICEmail actually processes the email contact.

5. Click **Ok** to close the **Status Properties** dialog box.

Configuring Avaya Content Analyzer (optional)

The IC server installation automatically installs Content Analyzer files on the server system. For more information, see Installing IC server components on page 35.

Before you can configure and use Content Analyzer, you must create and configure the Content Analyzer servers.

To configure Content Analyzer, perform the steps in the following topics:

1. Creating the Administrative Content Analyzer server on page 369
2. Creating the Operations Content Analyzer server on page 370

3. Adding a Knowledge Base on page 372

For more detailed information about Content Analyzer, see:

- *Avaya IC Workflow Designer User Guide* for an overview of Content Analyzer and information about how to customize workflows for Content Analyzer
- *Interaction Center Administration Guide* to administer Content Analyzer, including how to set up and maintain Knowledge Bases and how to train Content Analyzer

Creating the Administrative Content Analyzer server

For more information about the Administrative Content Analyzer server, see *Interaction Center Administration Guide*.

To create the Administrative Content Analyzer server:

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **CAAdmin** and click **Ok**.
3. On the **General** tab enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	CAADmin_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the IC domain for the server from the drop-down list.	This server should be in the same domain as the IC Email server. For example, select `Email` from the drop-down list if the server is in the Email domain.
Host	Select the IP address of the system from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Click the **CAAdmin** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
IC Data Source	Select the Interaction Center Data Source.	Select the default name: `interaction_center`.
Path to NLP Data	Enter the location of the NLP data.	Windows: *IC_INSTALL_DIR*\IC73\oem\banter\nlpdata Solaris: *IC_INSTALL_DIR*/IC73/oem/banter/NLPData/ AIX: *IC_INSTALL_DIR*/IC73/oem/banter/NLPData/ **Important:** Ensure that the path to the NLP Data is set as given above. If the path is not set correctly then the server will not start.

5. Click **Ok**.
6. Start the Administrative Content Analyzer server.

Creating the Operations Content Analyzer server

For more information about the Operations Content Analyzer server, see *Interaction Center Administration Guide*.

Note:
Do not start the Operations Content Analyzer server. You must configure at least one trained and validated Knowledge Base before you start this server.

To create the Operations Content Analyzer server:

1. In IC Manager, select **Server** > **New**.
2. From the list of servers, select **CAServer** and click **Ok**.

3. On the **General** tab enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	OperationCA_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the IC domain for the server from the drop-down list.	This server should be in the same domain as the IC Email server. For example, select `Email` from the drop-down list if the server is in the Email domain.
Host	Select the IP address of the system from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, IC Manager fills in the fields for Directory, Port, and Executable.

4. Click the **CA Server** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
IC Data Source	Select the Interaction Center Data Source.	Select the default name: `interaction_center`.
Path to NLP Data	Enter the location of the NLP data.	Windows *IC_INSTALL_DIR*\IC73\oem\banter\nlpdata Solaris: *IC_INSTALL_DIR*/IC73/oem/banter/NLPData/ AIX: *IC_INSTALL_DIR*/IC73/oem/banter/NLPData/ **Important:** Ensure that the path to the NLP Data is set as given above. If the path is not set correctly then the server will not start.
Knowledge Base	Select the Knowledge Base associated with this server.	Click the button to display the **Knowledge Base** dialog box. For more information, see Adding a Knowledge Base on page 372.

5. Click **OK**.

Adding a Knowledge Base

Before you add a Knowledge Base to your Operations Content Analyzer server, perform the following steps in the Content Analyzer Administration tab:

1. Create the Knowledge Base.
2. Train the Knowledge Base.
3. Validate the Knowledge Base.
4. Save the trained and validated Knowledge Base.

For detailed information on how to perform these steps, see *Interaction Center Administration Guide*.

You need the following information about the Knowledge Bases before you add them to the Operations Content Analyzer server:

- Name
- Knowledge Base file location
- Threshold
- Language codes

In IC Manager, the information for all the saved Knowledge Bases is available. You can find this information in the **KB Management** pane of the **Content Analysis** window.

To add a Knowledge Base to the Operations Content Analyzer server:

1. In IC Manager, select **Server** >**New**.
2. In the list of servers, double-click the operational CAServer.
3. In the **Server Editor** dialog box, click the **CAServer** tab.
4. Click the **Ellipsis (…)** button next to **Knowledge Base**.
5. In the **Knowledge Base** dialog box:
   a. Click **New**.
   b. Type the name of the Knowledge Base in the **Name** column.

      This name must be the same as the name of the Knowledge Base in the **KB Name** column of the **KB Management** pane in the **Content Analysis** window.

c. Type the directory path to the Knowledge Base in the **KB File Location** column.

   This path must be the same as the path in the **File Path** column of the **KB Management** pane in the **Content Analysis** window.

   If the Administrative Content Analyzer server and the Operations Content Analyzer server are hosted on the same physical system, this path must match the **File Path** column of the **KB Management** pane in the **Content Analysis** window.

   If the Administrative Content Analyzer server and the Operations Content Analyzer server are hosted on different physical systems, make sure that this file path accesses the same Knowledge Base as the one pointed to by the **File Path** column of the **KB Management** pane in the **Content Analysis** window.

d. Type a threshold in the **Threshold** column, if required.

   You can leave this column blank or type the same threshold that you specified when you validated the Knowledge Base.

e. Click the **Ellipsis** (**…**) button in the **Languages** column.

6. In the **Languages** dialog box:

   a. Click **New**.

   b. Type a language code.

      Repeat Steps a and b for each language code you want to add. All available language codes are in the **Languages** column of the **KB Management** pane in the **Content Analysis** window. The language codes are listed in a single string, separated by semicolons.

   c. Click **Ok**.

7. Click **Ok** in the **Knowledge Base** dialog box.

8. Click **Ok** in the **CAServer** tab.

Chapter 13: Configuring agent accounts

You must create and configure IC accounts for all agents who will use Avaya Agent, Avaya Agent Web Client, or a custom application developed using Client SDK.

After you create the agent accounts, you also need to configure:

- The Unified Agent Directory for agents who work with Avaya Agent
- The Address Book for agents who work with Avaya Agent Web Client
- The Address Book agents who work with custom applications created using Client SDK

With the Unified Agent Directory and the Address Book, agents can interact with other agents in the IC system.

Tip:
This section includes basic information about how to create test agents for a development IC system. A customized system or a production system may require that you configure additional properties. For more information about agent properties that you can configure for agent accounts, see *Interaction Center Administration Guide*.

This section includes the following topics:

1. Required permissions for agents on page 375
2. Cautions and tips for creating agent accounts on page 376
3. Creating an agent account on page 378
4. Setting agent properties on page 384
5. Configuring agents for Avaya Agent on page 386
6. Configuring agents for Avaya Agent Web Client on page 390
7. Creating agents for a Client SDK custom application on page 392
8. Configuring a Workflow server for transfers and conferences on page 395

Required permissions for agents

Agents can run IC agent desktop applications on their desktops with limited permissions over certain directories. Agents do not require administrator privileges.

Note:

If two different versions of Agent co-exist (for example, IC Agent 7.1 and IC Agent 7.3) on the same system, Agents should have the privilege of reading from and writing into Windows Registry. Agents should also have the privilege of running regedit.exe in silent mode.

The following table describes the permissions and allowable restrictions on IC directories for agent desktop applications.

Directory	Required permissions	Allowable restrictions
IC_INSTALL_DIR\IC73\bin	Modify permissions (includes Read, Write, Execute)	Delete
IC_INSTALL_DIR\IC73\etc	Modify permissions (includes Read, Write, Delete, Execute)	
IC_INSTALL_DIR\IC73\apps	Modify permissions (includes Read, Write, Delete, Execute)	
IC_INSTALL_DIR\IC73\logs	Modify permissions (includes Read, Write, Delete, Execute)	

Note:

In Windows 7, before running the qui.exe, ensure that the **Run as Administrator** option under compatibility mode for the qui.exe is unchecked.

Comments on this document? infodev@avaya.com

Cautions and tips for creating agent accounts

You must create an account in IC Manager for each agent, supervisor, and other employees who need to use IC. Each user account requires that you configure permissions, media channels, and other requirements.

This section contains information about creating agent and other user accounts for testing, including the minimal permissions and configuration settings. For more information, see *Interaction Center Administration Guide*.

This section also includes some important cautions and tips that you need to consider when you create agents for your IC system. For more information, see *Interaction Center Administration Guide*.

This section includes the following topics:

- Agent domains on page 376
- Agent workgroups and tenants on page 376
- Agent login IDs on page 377
- Agent password requirements on page 377

Agent domains

All IC agent accounts must belong to a User domain. You must create all User domains before you create your agents. If you have created agents first, you must assign all agents to the Default domain, and then create the User domains and reassign the agents.

If your User domain does not include a secondary ORB server, the domain must failover to a domain that includes an ORB server, such as the Default domain.

Agent workgroups and tenants

Organize your agent population into sets of tenants and workgroups that mirror the organization of your contact center.

A tenant is a set of workgroups that fulfil a particular business function. You can use tenants to define the security and administrative boundaries around data, queues, and content resources.

A workgroup is a set of agents or queues that form a logical grouping. A workgroup can only belong to one tenant. However, you can share agents across tenants by assigning them to multiple workgroups. To use workgroups, create workgroups and tenants before you create agents.

Tenants, workgroups, and agents inherit properties from parent to child entities. By default, if you assign a property value to a tenant, the workgroups in that tenant inherit that property value from the tenant, and the agents in the workgroups inherit the property value from the workgroups. When you assign agents to workgroups, and workgroups to tenants, you can specify the order of inheritance. The inheritance order controls which property value IC Manager uses for an agent if an entity inherits multiple values for the same property.

Agent login IDs

Each agent must have a unique login ID.

If an agent or supervisor needs to monitor multiple IC devices, the agent or supervisor must have a unique IC login ID for each device.

IC does not support simultaneous logins with the same login ID.

Important:
Simultaneous logins with the same login ID can cause serious issues with the performance of IC.

IC does not support:

- Two agents logging in with the same login ID.
- One agent simultaneously logging in to more than one system with the same login ID.
- One agent simultaneously logging in to more than one IC desktop application with the same login ID.

Agent password requirements

To prevent unauthorized access to IC, agents are assigned passwords that are required when they log in to IC.

Tip:
Password requirements (such as the required length and duration) are controlled by the properties in the Agent/Security section. For more information, see *Interaction Center Administration Guide*.

Creating an agent account

You must create at least one agent account to test the IC system and make sure that all features and media channels function correctly. When you create your production system, you must create an IC agent account for each agent who will work with an IC agent application.

Tip:
Create at least one agent in each User domain. Configure these agents to handle all applicable media channels.

The procedures in this section contain information on how to set basic properties for agent accounts, so you can test your system. If you want to set additional properties for your test agents, see *Interaction Center Administration Guide*.

To create an agent, perform the tasks in the following topics:

1. Creating an agent account on page 378
2. Configuring an agent for media channels on page 382

After you create an agent account, you must configure the agent properties, as described in Setting agent properties on page 384.

Creating an agent account

This procedure assumes that you will create the agent account in the Default tenant.

To create an agent account

1. In IC Manager, click the **Agent** tab.
2. In the left pane, expand the **DefaultTenant** node and select a tenant in that.

   If you want to create an agent account in a different tenant, select that tenant node in the left pane.
3. Select **Agent** > **New**.
4. Click the **General** tab and enter the information for the fields mentioned in the following table:

Field	Description
First Name	This is a required field. Type the agent's first name.
Last Name	This is a required field. Type the agent's last name.

Field	Description
Preferred Name	This is a required field. Type agent's preferred name.
Employee ID	Type the agent's company employee ID (if available).
Domain	This is a required field. Select a domain for the agent from the list. **Note:** If the agent handles chat contacts, the agent domain must failover to the domain that includes the Paging server.
Site	Select a site from the drop-down list. **Note:** IC uses the Site to compile statistics for groups, agents, or queues.

5. In the **System Information** group of the **General** tab, enter the information for the fields mentioned in the following table:

Field	Description
Login ID	This is a required field. Type a login ID that the agent uses for all IC applications. Each agent account must have a separate and unique login ID. For more information, see Agent login IDs on page 377.
Options	1. Click the **Ellipsis (…)** button next to **Options**. 2. Select the **User Addressable** check box to make the agents visible for transfers. 3. Click **OK**.

Field	Description
Task Load	This is a required field. Set the **Task Load** field to less than or equal to the sum of channel task loads. Use the arrow keys to set the maximum number of contacts that an agent can handle concurrently. These contacts can come from any of the media channels used by the agent. For example, if you plan to configure the test agent to use Email and Voice media channels, and to set the task load on Email to 2 and the task load on Voice to 1, set this Task Load property to 3.
Task Ceiling	This is a required field. The Task Ceiling is an upper limit on the Task Load. Use the arrow keys to set the limit of the task load across all of the media channels. The task load must be less than or equal to the task ceiling. **Note:** The Task Load can vary according to your system conditions, such as number of tasks, agents, or time of day.

6. In the **Membership Information** group of the **General** tab, enter the information for the fields mentioned in the following table:

Field	Recommended entry
Domain	This is a required field. Select your User domain from the drop-down list.
Workgroup	1. Click the **Ellipsis (…)** button next to **Workgroup**. 2. Expand the **DefaultTenant** node in the Workgroups list. 3. Select the **Default** workgroup. 4. Click **>>** to add the agent to the Default workgroup. 5. Click **OK**. **Note:** Agents can belong to more than one workgroup. Agents who work with chat contacts or email contacts must have the Default workgroup as their primary workgroup.
Site	Select a site from the drop-down list. **Note:** IC uses the Site to compile statistics for groups or agents or queues.

Tip:
If you want this agent to be a Supervisor, who can monitor chats between other agents and customers, configure this agent as the Supervisor for the Workgroup.

7. Click the **Email** tab in the center of the **General** tab, and enter the information for the fields mentioned in the following table:

Field	Recommended entry
Primary	Type the email address assigned to the agent by the contact center. This address is configured at the mail server. If you specify that the agent is user addressable on the System tab, IC lists this email address for the agent in the Agent Directory.
Internal	Type the email address assigned to the agent for internal email messages only. This address is not intended to be used outside of the contact center.
Personal	Type the email address assigned to the agent for personal, non-business communication from the agent.
Mobile Device	Type the email address assigned to the agent for use with their mobile device.

8. Click **Ok**.
9. Click the **Security** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry
Password	Type the password that the agent uses to log in to IC applications. For example, type agent1.
Confirm	Type the password a second time to confirm.
Roles	Select one or more check boxes to select the agent's security level.

10. Click **OK**.

Configuring an agent for media channels

When you set Task Load and Task Ceiling for the media channels, ensure that:

- The total of all Task Load values does not exceed the Task Load that you set for the agent on the **General** tab.
- The total of all Task Ceiling values does not exceed the Task Ceiling set on the **General** tab.

Important:
If you want an agent to handle Web Scheduled Callback contacts, you must configure the agent to handle voice and chat contacts.

This section includes the following topics:

- Configuring an agent to handle chat contacts on page 382.
- Configuring an agent to handle email contacts on page 383.
- Configuring an agent to handle voice contacts on page 383.

Configuring an agent to handle chat contacts

If you want the agent to receive and handle Web Scheduled Callback contacts, you must also configure the agent to handle voice contacts.

Tip:
This step continues from the previous step and assumes that the agent account remains open in IC Manager.

To configure an agent to handle chat contacts:

1. In IC Manager, click the **Channels** tab.
2. From the **Channel** drop-down list, select **Chat**.
3. Enter the information for the fields mentioned in the following table:

Field	Recommended entry
Disable Chat Channel	Clear this check box.
Task Load	Set the maximum number of chat contacts an agent can handle at one time.
Task Ceiling	Set the maximum value for the chat Task Load.

4. Click **Apply**.

Configuring an agent to handle email contacts

Tip:
This step continues from the previous step and assumes that the agent account remains open in IC Manager.

To configure an agent to handle email contacts

1. In IC Manager, click the **Channels** tab.
2. From the **Channel** drop-down list, select **Email**.
3. Enter the information for the fields mentioned in the following table:

Field	Recommended entry
Disable Email Channel	Clear this check box.
Show Full Headers	Select this check box if you want the agent to see the full header of each email contact.
From Address	Type the email address that you want recipients to see in emails from this agent.
Task Load	Set the maximum number of email contacts an agent can handle at one time.
Task Ceiling	Set the maximum value for the email Task Load.

4. Configure the primary email address for the agent, as described in Creating an agent account on page 378.
5. Click **Apply**.

Configuring an agent to handle voice contacts

If you want the agent to receive and handle Web Scheduled Callback contacts, you must also configure the agent to handle chat contacts.

Tip:
This step continues from the previous step and assumes that the agent account remains open in IC Manager.

To configure an agent to handle voice contacts:

1. In IC Manager, click the **Channels** tab.
2. From the **Channel** drop-down list, select **Voice**.

3. Enter the information for the fields mentioned in the following table:

Field	Recommended entry
Disable Voice Channel	Clear this check box.
Phone ID	Type the logical extension number for the agent's phone. For example, type 34181.
Password	Type the password for agent login to the ACD.
Phone Type	Type the type of phone that the agent uses. The switch requirement for agent login determines the phone type. Some supported switches support both phone types. Other supported switches only support one phone type. • Type EAS if the configuration controls the queue structure. You can only type EAS for Avaya DEFINITY/Communication Manager. • Type ACD if the switch requires a queue. You can type ACD for all supported switches.
Equipment	Type the physical extension number for the agent's phone. For example, type 24181.
Queue	Type the default voice queue for this agent.
Task Load	Set the maximum number of voice contacts an agent can handle at one time.
Task Ceiling	Set the maximum value for the voice Task Load.

4. Click **Apply**.

Setting agent properties

By default, IC provides default values for most agent properties. You can use these default values to ensure that the agent applications function correctly.

As you customize the IC system, you may need to configure different values for these agent properties. For example, you need to configure different values for the agent properties if you want the agent desktop applications to include wrapup functionality. For information about the agent properties or how to enable other features, see *Interaction Center Administration Guide*.

This section includes the following topics that describe how to set properties for agents:

• Setting global properties for all agents on page 385

- Setting properties for individual agents and workgroups on page 385

Setting global properties for all agents

The procedures in this topic assume that the property already exists in the property section. If a property does not exist, click **Add Property** and select that property from the **Assign Property** dialog box. For more information on adding properties to a property section, see *Interaction Center Administration Guide*.

To set global properties that affect all agents in IC:

1. In IC Manager, select **Tools** > **Groups**.
2. Click the **Properties** tab.
3. In the left pane, select the **IC** node.
4. In the **Sections** list, select the property section that includes the property you want to set.
5. In the right pane, double-click the property that you want to set.
6. In the **Edit Property** dialog box:
   a. In the **Property** drop-down list, verify that the correct property is selected.
   b. In the **Property Value** field, set the value for the property.
   c. Clear the **Descendants May Override** check box.
   d. Click **OK**.
7. Click **Apply**.
8. Click **OK**.

Setting properties for individual agents and workgroups

The procedures in this topic assume that the property already exists in the property section. If a property does not exist, click **Add Property** and select that property from the **Assign Property** dialog box. For more information on adding properties to a property section, see *Interaction Center Administration Guide*.

To set properties for individual agents and workgroups:

1. In IC Manager, click the **Agent** tab.
2. Select the required agent or workgroup:
   - To select a workgroup, navigate to and select the required workgroup in the left pane.
   - To select an agent, navigate to the workgroup that includes the agent in the left pane, then double-click the agent in the list of agents.

3. Click the **Properties** tab.
4. In the **Sections** list, select the required property section.
5. In the right pane, double-click the property that you want to set.
6. In the **Edit Property** dialog box:
   a. If necessary, select the property name from the **Property Name** drop-down list.
   b. In the **Property Value** field, set the value for the property.
   c. Clear the **Descendants May Override** check box.
   d. Click **OK**.
7. Click **Apply**.
8. Click **OK**.

Configuring agents for Avaya Agent

For agents who will work in Avaya Agent, these agent properties ensure that Avaya Agent and the Unified Agent Directory include the functions required by the agent. For example, you specify which Avaya Agent layout the agent will use.

For information about properties that configure additional features available for agents who work with Avaya Agent, including wrapup, see *Interaction Center Administration Guide*.

This section includes the following topics:

- Setting agent properties for Avaya Agent on page 387
- Configuring agents for the Unified Agent Directory on page 388

Setting agent properties for Avaya Agent

The agent properties that you must set for Avaya Agent include the Avaya Agent layout that an agent will use and the home directory for agents who handle chat contacts and email contacts.

You can change some or all of these default values to ensure that the functionality available to your agents matches the configuration of your Avaya IC system. Before you move to a production environment, review these properties to determine whether you need to change any of the default values. For more information about the additional agent properties, see *Interaction Center Administration Guide*.

Configuring the agent layout property

By default the agent layout property is configured for the out-of-the-box, English Avaya Agent layout. If the IC system includes a custom or non-English Avaya Agent layout, you must configure the Agent/Desktop/Layout property for that layout.

Configuring the home directory property

The home directory property is always configured from the perspective of Avaya Agent. The syntax that you use to configure the home directory property depends upon how the system that hosts Avaya Agent will access the directory. Since Avaya Agent is only supported on Windows, the syntax for the home directory must be in a format that Windows can use to access another network system.

Important:
Even if the home directory uses the same shared directory as the working directory, you may need to use a different syntax for the home directory property.

Note:
If the administrator has configured the shared path, `HomeDir,` for WebAgent in `Agent/Desktop/WAC`, then copy the folder's lexicons, images, and editlive to this path.

For more information about the home directory property, including recommended deployments of the home directory for Avaya Agent and the working directory of Avaya Agent Web Client, see *Interaction Center Administration Guide*.

To configure the home directory:

1. If it does not already exist, create the shared directory for the home directory on a network system.
2. Ensure that all agent workstations that host Avaya Agent:
   - Can access the shared directory for the home directory through either a mapped drive or UNC notation in Windows Explorer.

- Have the required Read, Write, and Execute permissions for that directory

3. Configure the `Agent/Desktop/WAC.HomeDir` as described in Setting agent properties on page 384.

   The following table provides examples of the syntax used to configure the home directory property. These examples use the `AgentResource` directory on a system named `resource.xyzcorp.com` as the shared directory.

Avaya Agent access to shared directory	Syntax for home directory
You map the Z: drive on each agent workstation to the shared directory folder hosted on a Windows network system. **Note:** Do not use this syntax if the shared directory is on a UNIX system.	`Z:\AgentResource`
Each agent workstation uses UNC notation in Windows Explorer to access the shared directory. **Note:** You can use this syntax if the shared directory is on a Windows or UNIX system.	`\\resource.xyzcorp.com\AgentResource`

Configuring agents for the Unified Agent Directory

The Unified Agent Directory contains resources for your contact center, including:

- Queues
- Agents
- Supervisors
- Subject Matter Experts
- Non-human resources, such as Interactive Voice Response units (IVRs)

You must configure queues and agents as Addressable if you want them to be visible in the Unified Agent Directory. For agents, set the ShowAgentsOnStartup property to be True to display the Directory tab in the Unified Agent Directory. Agents use the Directory tab to view individual agents in the contact center.

Agents can filter their view of the Unified Agent Directory to see only agents or queues that meet specified criteria. You can change this setting to force agents to view all of the agents and queues in your contact center, if required.

For information on how to set other properties related to the Unified Agent Directory, see *Interaction Center Administration Guide*. For information on how to use the Unified Agent Directory, see *Avaya Agent User's Guide*.

Note:

You do not need to perform these steps if the IC system does not include Avaya Agent.

The following table describes the properties that you need to set for agents to display in and use the Unified Agent Directory. All properties for the Unified Agent Directory are in the Agent/Desktop/Directory section.

Property	Recommended entry	Notes
ShowAgentsOnStartup	Yes	Adds the Directory Tab to the Unified Agent Directory.
ShowAgentState	Yes	Displays agent's state in the Directory tree of the Unified Agent Directory.
ShowAllAgents	Yes	Shows the entire Directory tree for agents in the Unified Agent Directory.
SkillsSupport	Yes	Lets agents use skills as search criteria in the Unified Agent Directory.
TransferFlowName	Type the name of the workflow that retrieves the destination from the virtual queue.	
WorkflowServerName	Name of the Workflow server that runs the workflows for the Unified Agent Directory.	Use the Workflow server where you added the semaphore in Configuring a Workflow server for transfers and conferences on page 395.
UADStringFormat	Select the required string format.	Determines how agents are displayed in the Unified Agent Directory. When you choose a string format, the Unified Agent Directory displays the following information in IC Manager: • Standard string format displays the Display Name for an agent. • ASCII string format displays the Full Name for an agent. • LoginID string format displays the Login Name for an agent.

Configuring agents for Avaya Agent Web Client

The only agent property that you must set for Avaya Agent Web Client is the working directory that an agent will use. IC Manager includes additional agent properties that have default values. You can change some or all of these default values to ensure that the functionality available to your agents matches the configuration of your IC system.

Before you move to a production environment, review the additional properties to determine whether you need to change any of the default values. For more information about the additional agent properties, see *Interaction Center Administration Guide*.

Tip:
You must also create a separate agent account for each Java Application Bridge that communicates with Avaya Agent Web Client. For more information, see Configuring an agent account for the Java Application Bridge on page 449.

This section includes the following topics:

- Configuring the working directory property on page 390
- Configuring agents for the Address Book on page 391

Configuring the working directory property

The working directory property is always configured from the perspective of Web Client Connector. The syntax that you use to configure the working directory property depends upon the operating system of the system that hosts Web Client Connector for Avaya Agent Web Client and how that system will access the shared directory.

Even if the working directory uses the same shared directory as the home directory, you may need to use a different syntax to configure the working directory property.

For more information about the home directory property, including recommended deployments of the working directory of Avaya Agent Web Client and the home directory for Avaya Agent, see *Interaction Center Administration Guide*.

CAUTION:
If you do not use a valid directory path when you configure the working directory, Avaya Agent Web Client will not function properly. Avaya Agent Web Client displays an error message on the Status Bar, and the chat and email channels will be disabled.

To configure the working directory:

1. If it does not already exist, create the shared directory for the working directory on a network system.

2. Ensure that all systems that host Web Client Connector for Avaya Agent Web Client:
   - Can access the shared directory for the working directory through one of the following methods:
     - A mapped drive or UNC notation in Windows Explorer
     - An NFS mount for the shared directory
   - Have the required Read, Write, and Execute permissions for that directory
3. Configure the `Agent/Desktop/WebClient.WorkingDirectory` as described in Setting agent properties on page 384.

   The examples in the following table use the `AgentResource` directory on a system named `resource.xyzcorp.com` as the shared directory.

Web Client Connector access to shared directory	Syntax for working directory
You map the Z: drive on the Web Client Connector system to the shared directory folder hosted on a Windows network system. **Note:** Do not use this syntax if Web Client Connector is on a UNIX system.	`Z:\AgentResource`
The Web Client Connector system uses UNC notation in Windows Explorer to access the shared directory. **Note:** Do not use this syntax if Web Client Connector is on a UNIX system.	`\\resource.xyzcorp.com\AgentResource`
You perform an NFS mount for the shared directory on the Web Client Connector system. **Note:** Do not use this syntax if Web Client Connector is on a Windows system.	`/opt/AgentResource`

Configuring agents for the Address Book

You do not need to configure any agent properties for the Address Book to work in Avaya Agent Web Client. However, if you want an agent to be visible in the Address Book, you must also configure the agent for the Address Book.

To configure agents for the Address Book in Avaya Agent Web Client:

1. Enable the **User Addressable** field in the **System Information** group of the **General** tab for each agent who:
   - Will work in Avaya Agent Web Client

- Must be visible in the Address Book

For more information on how to enable the User Addressable field, see Options in Creating an agent account on page 378.

2. Configure the primary email address for each agent who:
   - Will need to receive emails in Avaya Agent Web Client or from agents who work in Avaya Agent Web Client
   - Must be visible in the Address Book

   For more information, see Step 7 of Creating an agent account on page 378.

Creating agents for a Client SDK custom application

The only agent property that you must set for a custom application developed with the Client SDK is the working directory that an agent will use. IC Manager includes additional agent properties that have default values. You can change some or all of these default values to ensure that the functionality available to your agents matches the configuration of your IC system.

Before you move to a production environment, review the additional properties to determine whether you need to change any of the default values. For more information about the additional agent properties, see *Interaction Center Administration Guide*.

Tip:
You must also create a separate agent account for each Java Application Bridge that communicates with the Client SDK server. For more information, see Creating an agent account for the Java Application Bridge on page 473.

This section includes the following topics:

- Configuring the working directory property on page 390
- Configuring agents for the Address Book on page 391

Configuring the working directory property

The working directory property is always configured from the perspective of Tomcat. The syntax that you use to configure the working directory property depends upon the operating system of the system that hosts Tomcat for the Client SDK server and how that system will access the shared directory.

Even if the working directory uses the same shared directory as the home directory, you may need to use a different syntax to configure the working directory property.

For more information about the working directory property, including recommended deployments, see *Interaction Center Administration Guide*.

CAUTION:
If you do not use a valid directory path when you configure the working directory, your custom application will not function properly. You should configure your custom application to display an error message on the Status Bar and to disable the chat and email channels.

To configure the working directory:

1. If the working directory does not already exist, create the shared directory for the working directory on a network system.

   Note:
   For a working directory, if you create a shared directory on a remote system other than the SDK server or other than the system on which the **Avaya IC SDK Service 7.3** server is running, you must provide the necessary permissions to the Avaya IC SDK Service 7.3 service to access the remote system.

   To provide the access permissions, perform the following steps:

   a. From Windows Control Panel, double-click Administrative tools.
   b. Double-click the Services tool.
   c. In the services list, right-click the **Avaya IC SDK Service 7.3** service and select **Properties**.
   d. In the properties window, click the **Log On** tab.
   e. Select the **This account** option and enter the Administrator account name to access the remote system.
   f. Enter the valid password for the specified account.
   g. Click **OK**.
   h. Restart the **Avaya IC SDK Service 7.3** service.
   i. Close the Services tool window.

2. Ensure that all systems that host Tomcat for the Client SDK:
   - Can access the shared directory for the working directory through one of the following methods:
     - For a Windows system: a mapped drive or UNC notation in Windows Explorer
     - For a UNIX system, an NFS mount for the shared directory
   - Have the required Read, Write, and Execute permissions for that directory

3. Configure the `Agent/Desktop/WebClient.WorkingDirectory`.

   The following table provides examples of the syntax used to configure the working directory property. These examples use the `AgentResource` directory on a system named `resource.xyzcorp.com` as the shared directory.

Tomcat access to shared directory	Syntax for working directory
You map the Z: drive on the Tomcat system to the shared directory folder hosted on a Windows network system. **Note:** Do not use this syntax if Tomcat is on a UNIX system.	`Z:\AgentResource`
The Tomcat system uses UNC notation in Windows Explorer to access the shared directory. **Note:** Do not use this syntax if Tomcat is on a UNIX system.	`\\resource.xyzcorp.com\AgentResource`
You perform an NFS mount for the shared directory on the Tomcat system. **Note:** Do not use this syntax if Tomcat is on a Windows system.	/opt/AgentResource

4. Ensure that the **Avaya IC SDK Service 7.3** service running on the SDK server has the required permissions to access the remote system on which you created the shared location.

Configuring agents for the Address Book

You do not need to configure any agent properties for the Address Book to work in your custom application. However, if you want an agent to be visible in the Address Book of your custom application, you must also configure that agent for the Address Book.

To configure agents for the Address Book in your custom application:

1. Enable the **User Addressable** field in the **System Information** group of the **General** tab for each agent who:
   - Will work in your custom application
   - Must be visible in the Address Book

   For more information on how to enable the User Addressable field, see Creating an agent account on page 378.
2. Configure the primary email address for each agent who:

- Must receive emails in your custom application or from agents who work in your custom application
- Must be visible in the Address Book

For more information, see *Interaction Center Administration Guide*.

Configuring a Workflow server for transfers and conferences

For agents to be able to transfer or conference voice contacts and chat contacts to virtual queues, you must configure every Workflow server in a user domain for transfers and conferences. Without this configuration, agents will not be able to transfer contacts to queues and may encounter problems with transfers to and conferences with agents.

All IC systems require Workflow servers in User domains to handle agent transfers and conferences. You must perform these steps if the IC system includes Avaya Agent or Avaya Agent Web Client.

This section includes the following topics:

- Required configuration parameters on page 395
- Working with transfer workflows on page 396
- Configuring a Workflow server on page 396

Required configuration parameters

The following table describes the required configuration parameters for Workflow servers that handle agent transfers and conferences.

Configuration parameter	Value
Semaphore	agentsearch.update_searchresult
Synchronous Startup Flow	sys_transfer.update_vq_cache
Startup Flow	sys_agentsearch.update_agentstate_cache

Working with transfer workflows

The IC seed data includes these workflows. When you created the CCQ database, you imported the compiled workflows with the seed data and stored them in the database. However, you must still associate these workflows with the Workflow server.

Configuring a Workflow server

If your IC system includes multiple Workflow servers, perform these steps on every Workflow server in a user domain and every Workflow server that handles agent searches and transfers between agents.

Important:
If you create a new virtual queue or queue for agent transfers, you must do one of the following for every Workflow server in a user domains that runs workflows for the Unified Agent Directory:

- Manually run the sys_transfer.update_vq_cache workflow
- Restart each Workflow server

To configure the Workflow server for agent transfers and conferences:

1. In the **Server** tab of IC Manager, double-click a Workflow server in a user domain.
2. Click the **Workflow** tab.
3. Confirm that the Workflow server includes the following required semaphore: `agentsearch.update_searchresult`
   a. Click the **Ellipsis (…)** button next to **Semaphores**.
   b. If the rows do not include the required semaphore:
      - Click **New**.
      - In the new row, type **`agentsearch.update_searchresult`**
      - Click **Ok**.
4. Confirm that the Workflow server includes the required synchronous startup flows:
   a. Click the **Ellipsis (…)** button next to **Synchronous Startup Flows**.
   b. Verify that the rows include the following required synchronous startup flows:
      - `sys_transfer.update_vq_cache`
      - `sys_transfer.transfertovq`

      If the rows do not include either or both of those required flows, click **New** and add the missing flow.

5. Confirm that the Workflow server includes the following required startup flow:
   a. Click the **Ellipsis (…)** button next to **Startup Flows**.
   b. If the rows do not include the following required startup flow:
      `sys_agentsearch.update_agentstate_cache`
      - Click **New**.
      - In the new row, type **`sys_agentsearch.update_agentstate_cache`**.
      - Click **Ok**.
6. Click **Ok**.
7. Stop and restart the Workflow server.

   Repeat these steps for every Workflow server in a user domain.

Chapter 14: Deploying Avaya Agent

Perform the steps in the following topics to deploy Avaya Agent:

1. Required privileges for the agent installer on page 398
2. Creating installation files for agent applications on page 398
3. Preparing for installation by agents on page 404
4. Configuring WebAgent on page 408
5. Configuring the Citrix integration on page 419

Important:
Read the IC Release Notes and *Avaya IC Installation Planning and Prerequisites* before you install Avaya Agent.

Required privileges for the agent installer

All IC users who create agent installers and who install or configure IC components require an Administrator login or a login with administrator privileges.

Creating installation files for agent applications

To create installation files for agent applications, perform the steps in the following topics:

1. Cautions and tips for installation files on page 399
2. Required information for the Agent Site Preparation wizard on page 401
3. Running the Avaya Agent site preparation wizard on page 402
4. Copying the server implementation file on page 403

Cautions and tips for installation files

Before you run the Agent Site Preparation wizard, note the cautions and tips in the following topics:

- Disabling firewalls on page 399
- Stopping agent desktop applications on page 399
- Installation path for agent desktop applications on page 400
- Size of agent installer directory on page 400
- Installer directory availability on page 400
- Location for Avaya Agent installation on page 400
- Size of Avaya Agent installation directory on page 400
- Solaris system on page 400
- AIX system on page 400

Disabling firewalls

If the system where you want to install Avaya Agent has a personal or desktop firewall, you need to disable the firewall before you start the installation. You can re-enable the firewall after the installation is complete.

Stopping agent desktop applications

Before you or an agent runs the Agent Installer on an agent desktop system, confirm that there are no IC agent desktop applications or qui.exe processes running on the agent desktop system. The Agent Installer may stop responding or pause indefinitely if an agent desktop or qui.exe process is still running.

Configuring Internet Explorer on agent workstations

Set the following internet options in Internet Explorer for all agents who will handle chat contacts:

- Security level: Medium if agents use Microsoft Windows XP, Windows Vista, Windows 7, and Windows 8.1.
- ActiveX controls: allow to run.
- Trusted sites: add the URL of the Website server to the Trusted Sites list.

Installation path for agent desktop applications

The agent installer automatically adds the following to the installation path for agent desktop applications: `\apps\<application_name>`

When you specify the initial section for the installation path, do not include any duplication of the directories. If you include a duplicate directory, the `-d` parameter in the shortcut cannot find the working directory for the applications.

For example, if you specify `C:\apps` as the installation path for agent desktop applications, the `-d` parameter cannot locate the apps directory, as it is duplicated in the installation path of `C:\apps\Avaya\IC73\apps\interaction_center`

Size of agent installer directory

Select a network share with at least 110MB of available disk space for each agent installer directory.

Installer directory availability

Make sure that the network system is online when you run the Agent Site Preparation wizard.

Location for Avaya Agent installation

Select the directory path for the Avaya Agent installation on the desk top systems.

Size of Avaya Agent installation directory

Make sure that the agent desktop systems have at least 350 MB of available disk space. Approximately 220 MB of the required available space must be in a `temp` directory. The agent installer deletes the files in the `temp` directory when you reboot the agent desktop system.

Solaris system

If you plan to host the agent installer on a Solaris system, you must:

1. Run the Agent Site Preparation wizard on a Windows system.
2. Transfer the files to a Samba share on the Solaris system.

AIX system

If you plan to host the agent installer on an AIX system, you must:

1. Run the Agent Site Preparation wizard on a Windows system.
2. Transfer the files to a Samba share on the AIX system.

Required information for the Agent Site Preparation wizard

Before you complete the required information, you must know how many different agent configurations your contact center requires. If you must create multiple agent configurations, you must run the Agent Site Preparation wizard for each configuration.

You must plan your agent desktop configuration before you run the Agent Site Preparation wizard. The tables in each section provide examples of the kind of planning and information that you must complete before you run the Agent Site Preparation wizard. You can fill out your configuration information in these tables, or create similar tables of your own.

Path for agent installers: The path for agent installers specifies the directory path for the folder where you place the agent installer and configuration data for each agent configuration.

The default directory is: `C:\Avaya\IC73\AgentInstaller`. You can copy the installation files to another location, such as a Web server, after you create the agent installer.

By default, the Agent Site Preparation Wizard places the agent installer in a directory path that includes *IC73* to ensure that you do not overwrite an earlier version of the agent installer. The default directory path is `C:\Avaya\IC73\AgentInstaller`.

Directory on agent desktop: The directory on the agent desktop specifies where the agent installer will install Avaya Agent. Use a drive and directory that is valid on all agent desktop systems. The agent installer will present this directory to all agents during the installation. If required, you can let agents override the default installation directory and select their own installation directory.

By default, the agent installer places the agent desktop applications in a directory path that includes *IC73* to ensure that the agent applications are correctly updated.

For example, the default directory and path for installing agent desktop applications is: `C:\Avaya\IC73\`.

Applications to be installed: Most Avaya Agent installations use Interaction Center as the agent application to include in each agent configuration.

Telephony switch type: If your IC system includes Telephony, you must know the type of telephony switch used by the agents who use the version of Avaya Agent installed by this agent installer.

Automatic updates: Automatic updates configure Avaya Agent to update agent configurations to the latest version whenever agents log in.

Running the Avaya Agent site preparation wizard

Repeat this entire procedure for each Avaya Agent configuration in the IC system.

To run the Avaya Agent site preparation wizard:

1. Insert IC Release 7.3 CD/DVD-ROM 4.

   The IC installer starts automatically. If you disabled Autorun on the system, navigate to the Servers directory on the CD/DVD-ROM and run `setup.exe`.

2. When the IC installer opens, read the entire IC license agreement carefully, then accept the terms of the agreement. Select **Next**, then follow the prompts in the installer.

   The IC installer exits if you do not agree to the terms of the agreement.

3. In the product installation screen, select **Avaya Rich Client Preparation Wizard** 7.3. Select **Next**, then follow the prompts in the installer.

4. In the Avaya Agent installation folder screen:

   a. Accept the default or type the path to the directory where the agent installer will install the application files on each agent desktop.

   b. Select one of the options in the following table:

Option	Description
Yes, allow agents to choose an alternate folder	Allows agents to decide where to install Avaya Agent.
No, always use the pre-defined folder	Does not allow agents to decide where to install Avaya Agent. If you select this option, Avaya Agent will always be installed in the same folder on the agent desktop.

   Note:
   Do not use `apps` in the installation path for agent desktop applications. If you do, the `-d` parameter cannot locate the apps directory and start the application.

   c. Click **Next**.

5. In the applications screen:

   a. Select the following application for agents who use this configuration:

   - interaction_center

   If you plan to use Avaya Agent only, select interaction_center.

b. Select one of the options in the following table:

Option	Purpose
Yes, allow Avaya Agent to perform updates automatically	To have Avaya Agent automatically check for and apply updates each time an agent logs in.
No, updates will be done manually	To require agents to apply updates manually when you notify them that an update is available.

c. Select **Next**.

6. In the telephony switch window, select the type of phone switch to use with Avaya Agent.

   If this configuration does not include Telephony, select **None**.

7. Select **Finish** to complete the agent installer.

Copying the server implementation file

The agent installer requires access to the `vesp.imp` server implementation file from the system that hosts the primary ORB server. You must copy this file to a location where the agent installer has access.

To copy the server implementation file:

1. Navigate to the following directory where the vesp.imp file is located:

   IC_INSTALL_DIR\IC73\etc

2. Copy the `vesp.imp` file to the following directory on the system that hosts the agent installer:

   IC_INSTALL_DIR\IC73\AgentInstaller\config

Note:
Do not copy the `vesp.imp` file to the *IC_INSTALL_DIR*\IC73\bin directory. The `vesp.imp` file cannot function properly from this directory.

Preparing for installation by agents

As you complete these procedures, refer to the following table for the directories and files in the Avaya Agent installer directory.

Directory	Contents
<*agent_installdir*>\config	This directory contains the files that agents install to update Avaya Agent.
<*agent_installdir*>\update	This directory contains updates that you make available to the agent applications.
<*agent_installdir*>\install.exe	The executable that runs the installation of an agent configuration on the agent desktop.

To prepare an agent installer for installation by agents, perform the steps in the following topics:

1. Testing the agent installer on page 404
2. Creating installation instructions for agents on page 405

Testing the agent installer

You must test the agent installer to make sure that:

- The agent installer works properly.
- The correct installation options are available for agents when they install the agent configuration.
- The agents can access the agent installer through a shared network drive.

Note:

Before you install IC agent applications, configure all agent workstations with restore points. The agent installer replaces some system files during the installation. If software conflicts arise, restore points allow easy rollback after you uninstall IC. See the Windows documentation or third-party guides for procedures on enabling such functionality.

If you placed the agent installer on a shared network drive, agents can copy the folders to their systems, or run the agent installer across the network.

If the agents run the agent installer across the network, they must be able to access the shared network drive from their systems. Agents cannot use the **Run** dialog box on the **Start** menu to run the agent installer.

To test the agent installer:

1. Close down all Windows applications.
2. Use Windows Explorer to navigate to the folder, then right-click **install.exe**, and select **Run as Administrator**.
3. When the Avaya Agent installer opens, read the entire IC license agreement carefully, then accept the terms of the agreement: Select **Next**, then follow the prompts in the installer.

   The Avaya Agent installer exits if you do not agree to the terms of the agreement.

Note:

The following error message can occur:

You must use "Turn Windows features on or off" in the Control Panel to install or configure Microsoft .Net Framework 3.0 x86.

Click **Ok** on the message window to proceed further.

Note:

The **Visual C++ Redistributable Installation** dialog box appears. Click **Yes** to install the Visual C++ runtime libraries. VCRedist is a Microsoft re-distributable package ‘Visual C++ 2005 SP1(MFC security update)’ that installs Visual C++ runtime libraries required to run IC. If Visual C++ 2005 SP1 or a later is already installed by another application, this installation can be skipped. Click **No** to skip VCRedist package installation.

4. After the Avaya Agent installer completes:
   a. Select **Yes, restart my computer**.
   b. Select **Finish**.

   After the system reboots, the installer registers all necessary DLLs and OCXs.

Creating installation instructions for agents

Follow these steps to send the URL or directory path and other instructions to all agents who must install a specific agent configuration.

Create instructions for agents that include the following:

- Directory path to the network drive.
- Instructions to close all applications before starting the installation.

- Any other special instructions, such as whether they can select their own installation directory.
- The name of a person to contact if they have problems.

Configuring automatic updates for agent applications

IC allows you to make different types of updates to agent desktop applications. If you enable more than one type of update, IC applies the updates in the following order:

1. Language pack updates that install updated language packs for all supported languages.
2. Service pack updates that install updated application files on the agent desktop.
3. Point patch updates that install patch updates to the application files.

Note:
For any type of automatic update to work correctly, the agents must have Read access to the `version.html` file and to the updates. For example, if you install the language pack update on a network server, each agent that logs in must have Read permissions for the directory.

If you enabled Automatic Updates in the Agent Site Preparation wizard:

1. When an agent logs in, IC reads the `version.html` file from `<agent installdir>\config`.
2. If the following is true, then IC invokes the automatic updates:
   - Value of `icagent` in the `version.html` file is "1"
   - Values for `majorversion` and `minorversion` in the downloaded `version.html` file on the agent desktop system match the values in the agent registry
   - Values for `patchversion`, `servicepackversion`, or `languagepackversion` are greater than the values in the agent registry
3. When the automatic update is invoked:
   a. A message is displayed to the agent.
   b. The agent application exits.
   c. IC updates the agent applications on the agent desktop.

This section contains the following:

- Updating the version.html file on page 407
- Temporarily disabling automatic updates on page 408

Updating the version.html file

You must update the `version.html` file in the agent installer directory with new values to invoke automatic updates of the agent applications. The `version.html` file contains the following fields. You can update the highlighted section.

```
<versioninfo>
  <remote>
    <client>
      <icagent enabled="1" majorversion="6" minorversion="0" patchversion="0"
      patchpath="%VALUE%" servicepackversion="0" servicepackpath="%VALUE%"
      languagepackversion="0" languagepackpath="%VALUE%"/>
    </client>
    <server>
    </server>
  </remote>
  <local>
    <client>
      <icagent regkeyname="Agent"/>
    </client>
    <server>
    </server>
  </local>
</versioninfo>
```

To update the version.html file:

1. Open the `version.html` file in a text editor.
2. In the `version.html` file, increase the value of one or more of the fields as shown in the following table by one. For example, if the value of a field is currently 1, increase the value to 2.

Field	Purpose
languagepackversion	Increase the value of this field for a language pack update.
servicepackversion	Increase the value of this field for a service pack update.
patchversion	Increase the value of this field for a patch update.

Do not change the `majorversion` and `minorversion` values unless specifically instructed.

3. In the `version.html` file, type the location of the agent installer files in one or more of the following fields. The shared network directory or Web site must be available from the agent desktop.

Field	Purpose
languagepackpath	Type the location in this field for a language pack update.
servicepackversion	Type the location in this field for a service pack update.
patchversion	Type the location in this field for a patch update.

   IC checks this field before it downloads the files from that location. If the URL or network directory is not valid, an error message is displayed to the agent. After the agent selects **OK**, the agent applications are launched without being updated.

4. Save the `version.html` file.
5. Repeat these steps for every Avaya Agent configuration.

Temporarily disabling automatic updates

In some cases, you may want to disable your Automatic Update option temporarily and allow agents to log in without waiting for the Automatic Update to complete.

To disable Automatic Updates:

1. Open the `version.html` file in the `<agent_installdir>\config` directory.
2. Change the value of the `icagent enabled` field to 0.
3. Save the file.

Configuring WebAgent

You can configure the WebAgent by specifying the values for different parameters in the `Application.properties` file. You can find the `Application.properties` file in the home directory that you have specified in IC Manager.

This section contains the following:

- Locating Application.properties file on page 409
- Configuring the location to write the webagent logs on page 409
- HTML Editor configuration for Rich Client on page 410

- Configuring Avaya Agent to convert an email message to an attachment on page 412
- Configuring auto flush on page 412
- Configuring number of attachments to be displayed without scrollbar on page 412
- Configuring the default location for saving attachment on page 413
- Configuring default sorting on page 414
- Configuring UTF-8 Encoding on page 414
- Configuring Avaya Agent to populate Email templates on page 414

Locating Application.properties file

You can create the Application.properties file in the home directory and specify the location of that file in the **HomeDir** property in IC Manager.

Note:
You must create the **Application.properties** file in the home directory, if it does not exist.

To specify the location Application.properties file in IC Manager:

1. In IC Manager, select **Tools** > **Groups**.
2. In the left pane, select **IC**.
3. In the right pane, click the **Properties** tab.
4. In the **Sections** list, select **Agent/Desktop/WAC**.
5. Edit the **HomeDir** property to specify the home directory location.

Configuring the location to write the webagent logs

Webagent uses the agent working directory defined in the ICManager to write the logs. If the working directory is on the network share for example some shared folder on a different system, then the webagent uses the shared folder over network to write each log statement. If there is a network latency and the log level specified in the ICManager for the webagent is set to the debug level-15 then writing the log over the network causes the webagent to have lag while rendering the chat transcipts.

You can configure the webagent to write the logs on the local agent computer or on the network share. By default, the "**application.trace.local=**" parameter is set to false. If you set this parameter to true, then the webagent writes the logs on the local disk of the agent machine even if the agent working directory is specified on the network share. The location for the logs written on the local disk of the agent machine is: <Agent_Home_Directory>/webagent/logs.

If the webagent working directory is on the network share, then this parameter need to be added in the Application.properties file present in the agent working directory (network share).

To configure Web agent to write log files to the local agent computer:

1. Replace or add the following key in the **Application.properties**:

   application.trace.local=`true`

HTML Editor configuration for Rich Client

When you install IC Rich Client, a new folder "..\IC73\WebAgent\editlive" is created. This folder will contain the following xml configuration files:

- NewOutboundEmail.xml
- PreviewEmailConfig.xml
- ReplyForwardEmailConfig.xml
- ResourcesConfig.xml

The above files contain the configuration parameters to configure the text plain/Html properties for specific functions as the name of the xml suggests.

Application.properties file: This file contains a property to Enable/Disable the editor logging using the property email.editor.log.level. By default, this property is disabled. The default value is email.editor.log.level=false

This property can be used to debug the editor.

Important:
If the Shared Path "HomeDir" for WebAgent is configured in ICManager, using the property "Agent/Desktop/WAC", then copy the folders lexicons, images, and editlive under this path.

The following properties of Application.properties file are deprecated:

- email.edit.defaultNewFont
- email.edit.defaultNewFontSize
- email.edit.defaultReplyFont
- email.edit.defaultReplyFontSize
- email.HtmlNewMessage.r
- email.HtmlNewMessage.g
- email.HtmlNewMessage.b
- email.HtmlReplyMessage.r
- email.HtmlReplyMessage.g

Since AIC 7.3.9 HTML editor is configured by *.js configuration files, which created from *.xml file in a same folder at first creating HTML editor. After any changes in *.xml files eponymous *.js file should be deleted, for changes to take place.”

2) In item “HTML Editor configuration for Rich Client.

Since AIC 7.3.9 attributes under section <wysiwygEditor> are deprecated.”
3) In item “WebAgent HTML Editor

Configuring Avaya Agent to convert an email message to an attachment

You need to configure the Avaya Agent to convert large size email messages to an attachment. With this configuration, the Avaya Agent converts a large size email message to an attachment with file name as `message.txt` (for plain text message) and `message.html` (for html text message).

To configure avaya agent to convert large size email messages to an attachment:

1. Replace or add the following key in the **Application.properties**:

   ```
   email.largeemail.putasattachment=true
   email.largeemail.size=<In KB>
   ```

Configuring auto flush

You need to configure the Avaya Agent to flush log messages to the `webagent.log` file.

To configure auto flush:

1. Replace or add the following key:

   ```
   application.trace.flush=true
   ```

Note:
By default, Auto flush is false.

Configuring number of attachments to be displayed without scrollbar

You need to configure the number of attachments to be displayed without scrollbar in the WebAgent.

To configure the number of attachments:

1. Replace or add the following key:

   ```
   email.attachment.length=<number of attachments>
   ```

Note:
The default number of attachments is set to 20.

Configuring the default location for saving attachment

You need to configure the Avaya Agent to change the default location for saving attachments in the WebAgent.

To configure the attachment location:

1. Replace or add the following key:

   ```
   default.attachment.location=\\\\<Location_to_store_attachments>
   ```

Note:

If this location is accessible and if the specified directory does not exists, a new directory with the name of an agent is created. Attachments are stored at the specified location for that particular agent.

If this location is not accessible, then the attachments are stored at the following location:

```
...\IC73\WebAgent\attachments
```

Or

```
\\<Shared_Root_Directory>\attachments
```

Configuring default sorting

You need to configure the Avaya Agent to set the default sorting column for Customer History and Tracking History.

To configure the default sorting column:

1. Replace or add the following keys:
   - For Customer History:

     `history.customer.column.sort=<column_no>`
   - For Tracking History:

     `history.tracking.column.sort=<column_no>`

Configuring UTF-8 Encoding

You need to configure the Avaya Agent to detect incompatible character set encodings and use UTF-8 character set for outbound email.

To configure UTF-8 Encoding:

1. Replace or add the following key:

   `email.charsetdetection.coverttoutf8=true`

Configuring Avaya Agent to populate Email templates

You need to configure the Avaya Agent to populate the subject line and attachments of Email templates:

To configure viewing Email templates:

1. Replace or add the following keys:

   `email.template.preview.level=3`

   `email.template.use.level=3`

   `emailresource.usage.subject.behavior=3`

Key	Value
email.template.preview.level	Do not change the value.
email.template.use.level	Do not change the value.
emailresource.usage.subject.behavior	The default value is 1. • If you set the value to 1, the subject is not copied. The subject is kept as per the existing subject. • If you set the value to 2, the subject overwrites existing subject in email. • If you set the value to 3, the subject is added to existing subject in email before the existing subject. • If you set the value to 4, the subject is added to existing subject in email after the existing subject.

WebAgent HTML Editor

The user interface and behavior of the WebAgent HTML editor can be configured using the EditLive! configuration XMLs. These XMLs contain the configuration data which is used by Ephox Editlive! to render the UI and respond to UI events.

Out of the box, the following four configuration XMLs are provided to customize the UI and features of the WebAgent HTML editor:

NewOutboundEmail.xml: This is used for rendering the UI for new email composition in HTML mode.

PreviewEmailConfig.xml: This is used for previewing the email in HTML mode.

ReplyForwardEmailConfig.xml: This is used for rendering the UI for email composition in reply/reply all/forward in HTML mode.

ResourcesConfig.xml: This is used for rendering the UI for resource related operation e.g. edit/preview in HTML mode.

Since AIC 7.3.9 WebAgent uses TinyMCE HTML editor. It is configured by eponymous *.js configuration files. WebAgent when necessary generates them. *.js files should be deleted for any changes in *.xml file to take place in TinyMCE editor

This section contains the following:

- Hyperlink settings in Configuration XML on page 416

- Configuring Hyperlink dialog box for HTML Email on page 418

Hyperlink settings in Configuration XML

With the Hyperlink dialog box you can specify the link type and target location for a hyperlink jump to be encoded around the string or image selected in your document.

This section contains the following:

- Displaying Hyperlink button in toolbar on page 416
- Configuring Insert Hyperlink dialog box on page 416

Displaying Hyperlink button in toolbar

To display the hyperlink control for the HTML Editor toolbar, the following tags are used in the configuration file:

- <toolbars>: This element contains the configuration information for the toolbars within EditLive!. This includes the Format and the Command toolbars and the buttons and combo boxes contained within them.
- <toolbar>: This element contains the configuration information for a toolbar for use within EditLive!.
- < toolbarButton>: This element causes a particular button to be present on the toolbar within EditLive!.

```
<!--      Customize the EditLive! toolbars
-->
    <toolbars>
        <toolbar name="Format">
.
.
  <toolbarButton name="HLink"/>
        </toolbar>
    </toolbars>
```

In the above snippet, the <toolbarButton> tag is used to insert the Hyperlink button in the HTML 'Format' toolbar.

Configuring Insert Hyperlink dialog box

The **Insert Hyperlink** dialog box can be customized for links and email ids using following tags:

- <hyperlinks>: This element allows for the configuration of a list of hyperlinks and e-mail addresses to be made available to the end users of EditLive! using the Insert Hyperlink dialog.
- <hyperlinkList>: This element allows for the specification of a list of hyperlinks that the users of EditLive! will be provided using the Insert Hyperlink dialog.

- <mailtoList>: This element allows for the specification of a list of e-mail addresses that the end users of EditLive! will be provided using the Insert Hyperlink dialog.
- <PlacesInDocument>: This element allows the "Places in Document" panel of the Insert Hyperlink dialog to be hidden.

Fields:

The **Insert Hyperlink** dialog box contains the following fields and options:

URL: specifies URL address of a link.

Text to Display: Specifies a description for the hyperlink. This is useful when the file name or URL is not helpful in identifying the contents of the linked file.

Title: Specifies text that appears when the user's pointer is over a hyperlink.

Link list: dropdown list with predefined links and e-mails. Will not appear, if no links were defined in configurational files."

.

Configuring Hyperlink dialog box for HTML Email

The **Hyperlink** dialog box can be configured to display the default Web Links and Email Address, which can be used for hyper linking any text inside the WebAgent HTML Editor.

Modify the Editlive! configuration files to enable default Web-Links and Email addresses:

1. Go to <AVAYA_IC73_HOME>\IC73\WebAgent\editlive directory on the system where AARC is installed.
2. Edit the file NewOutboundEmail.xml.
3. Go to "<hyperlinks>" tag.
4. Uncomment <hyperlinkList> and <mailtoList> tag..
5. To customize the hyperlinks and email ids, provide appropriate values for "href" and "description" attributes in <hyperlink> and <mailtolink> tags.
6. Follow steps 1 to 5 for the following files:
   - <AVAYA_IC73_HOME>\IC73\WebAgent\editlive\ReplyForwardEmailConfig.xml
   - <AVAYA_IC73_HOME>\IC73\WebAgent\editlive\ResourcesConfig.xml

Note:

Copy the changed configuration files to the respective "WAC/HomeDir" if it is other than the default Home Directory defined in ICManager.

Configuring the Citrix integration

The Citrix client interface with the seamless window causes issues with the login behavior and the appearance of the IC agent desktop applications. Avaya provides two tools that prevent these potential issues. For more information, see *Avaya IC Installation Planning and Prerequisites*.

You do not need to perform additional steps if the IC uses the Citrix Web interface.

For this configuration, the Citrix integration requires some additional steps to ensure that the agents can connect to the agent desktop applications and that the agent desktop applications function correctly in the Citrix interface.

This section includes the following topics:

- About the Citrix integration on page 419
- Installing the agent applications on the Citrix server on page 420
- Deploying Avaya Agent Rich Client on the Citrix server on page 429
- Locating the files for the tools on page 431
- Configuring the Avaya Agent INI file on page 432
- Configuring the IC Web browser tool on page 433
- Configuring the executable tool on page 436
- Sequence for using the Avaya tools for Citrix on page 440
- Creating ICA (Citrix Client) connection with Citrix server on page 441

For more detailed information about the IC tools and the Citrix integration with IC, see *Avaya IC Installation Planning and Prerequisites*.

About the Citrix integration

IC supports the following methods of publishing applications in Citrix:

- Agent applications accessed as embedded applications in the Citrix Web interface.
- Agent applications accessed in a seamless window in the Citrix client interface.

This section includes the following topics:

- Limitations of Citrix integration with IC on page 420
- Configuring Citrix integration for seamless window applications on page 420

Limitations of Citrix integration with IC

Before you deploy your IC agent desktop applications on a Citrix server, consider the following limitations:

- Do not host embedded applications and seamless window applications on the same Citrix server. To use both publishing methods in an IC system, host the embedded applications on a different Citrix server from seamless window applications.
- Do not use the Web browser tool, the Executable tool, or the Avaya Agent INI file (qui.ini) on a Citrix server that hosts embedded applications.

Configuring Citrix integration for seamless window applications

If the IC system includes access to IC agent desktop applications through the Citrix client interface in a seamless window, you can configure the Citrix integration in the following ways:

- Configure and run the Web browser tool to access the agent desktop applications.
- Configure and run the Executable tool to access the agent desktop applications.

Installing the agent applications on the Citrix server

To install the agent desktop applications on a Citrix server, follow the procedures in Testing the agent installer on page 404. Do not perform any additional steps during the installation.

Depending upon the environment, you may need to adjust the size of the Avaya Agent framework, and then re-create the agent installer. For more information on how to customize the framework size, see *Avaya Agent Integration*.

Note:

You cannot install the agent desktop applications in a Citrix environment if you do not select the Citrix installation option in the Agent Site Preparation Wizard. For more information, see Running the Avaya Agent site preparation wizard on page 402.

Deploying Citrix Xenapp 7.5

This section contains the following:

- Installing Citrix XenApp 7.5 on page 421
- Configuring the XenApp 7.5 Site on page 423
- Configuring the Virtual Delivery Agent software on page 424

- Creating machine catalog on page 426
- Configuring the Delivery group on page 427
- Displaying or modifying the application properties on page 428

Installing Citrix XenApp 7.5

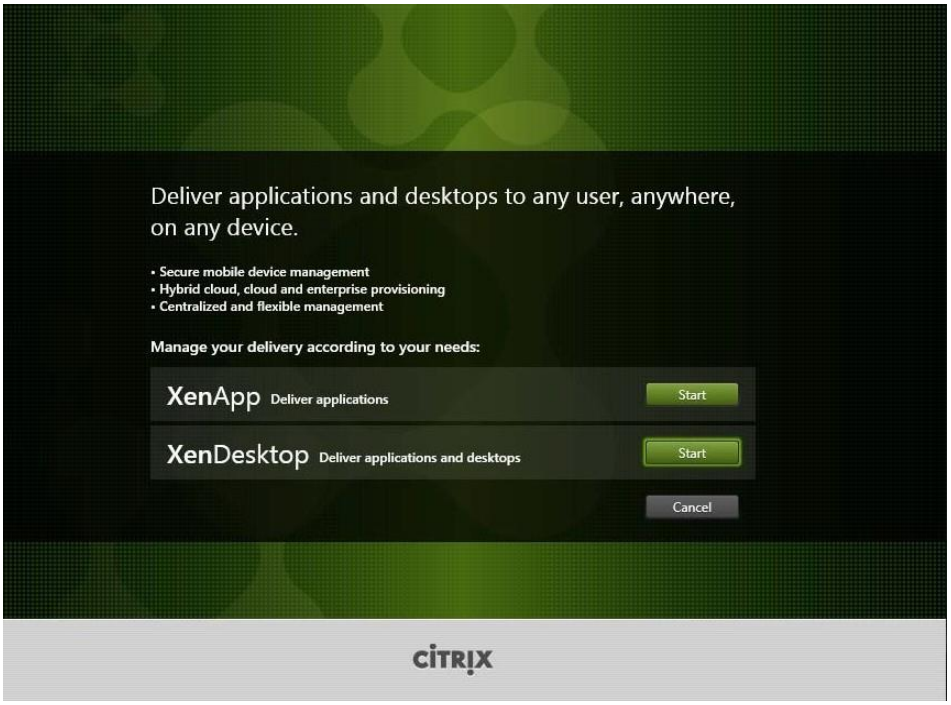
The Citrix installation source comes with the single setup application for installing XenDesktop and XenApp.

To install Citrix XenApp 7.5:

1. Log in to the server.
2. Double-click the AutoSelect.exe file.

   The system displays a window with the following deployment option:

   - XenApp
   - XenDesktop



3. On the **XenApp Deliver applications** option, click **Start**.

   There are options for installing the following:

- In the left pane, under **Get Started**, **Delivery Controller**. This option installs the Delivery Controller and other essential services like License Server and StoreFront. Citrix Delivery Controller for initial Citrix XenApp environment setup.
- In the center pane, under Prepare Machines and Images:
  - Virtual Delivery Agent for Windows Server OS: This option is used to install agent to deliver applications and desktops from server-based VMs or physical machines.
  - Virtual Delivery Agent for Windows Desktop OS
- In the right pane, under Extend Deployment the following options are available:
  - Citrix Director
  - Citrix License Server
  - Citrix StoreFront
  - Citrix Studio
  - Universal Print Server

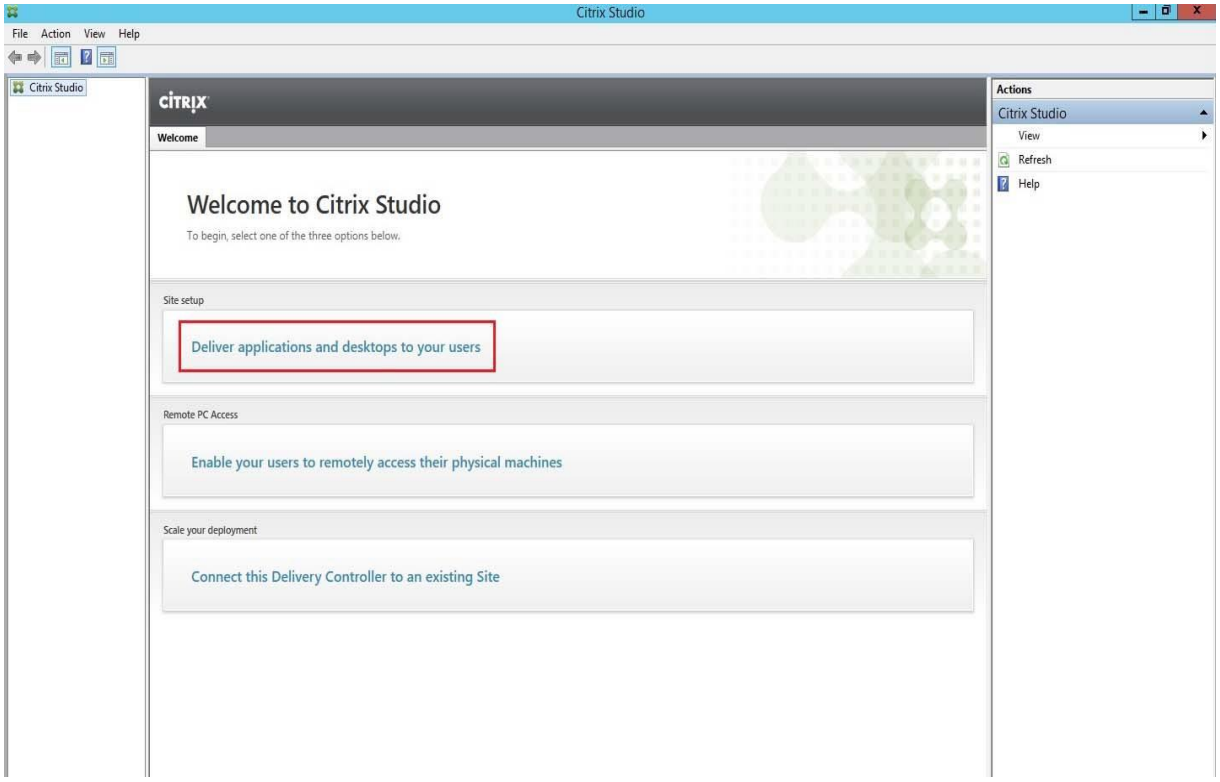
4. On the **XenApp 7.5** window, in the left pane, click **Deliver Controller**.
5. In the **Software License Agreement** screen, click **I have read, understand, and accept the terms of the license agreement**.
6. Click **Next**.
7. In the **Core Components** screen, select the following options.
   - Delivery Controller
   - Studio
   - Director
   - License Server
   - StoreFront
8. Click **Next**.
9. In the **Features** screen, select the following options:
   - **Install Microsoft SQL Server 2012 Express** for Datastore
   - **Install Remote Assistance** for shadowing the client session from Director.

   Note:
   If you do not select SQL Server 2012 Express for Datastore you must have a SQL server separately.
10. Click **Next**.
11. In the **Firewall** screen, click **Next**.
12. In the **Summary** screen, click **Install**.
13. In the **Finish Installation** screen, click **Finish**.

Configuring the XenApp 7.5 Site

To configure the XenApp 7.5 Site:

1. Log in to the server.
2. Open the Desktop Studio application.
3. On the **Welcome to Citrix Studio** screen, click **Deliver applications and desktops to your users**.



The system displays the **Site Setup** window.

4. On the **Introduction** screen:
   a. Under the **What kind of Site do you want to create?** section, keep the default value.
   b. Under the **Site name:** field, provide a site name.
5. Click **Next**.
6. On the **Database** screen, the wizard populates the standard database name based on the site name created in the previous step.
7. Click **Next**.
8. In the **Studio** dialog box, Click **OK** to create a database automatically.

9. In the **Licensing** screen provide the licensing server information. Enter a license server name or leave the default settings on licensing page. A 30-day trial license is included in the installer. If you already have a license server, provide the details of the license server and select the appropriate product.
10. Click **Next**.

    The system displays the Summary page. Review the Site Setup information.
11. Click **Finish** to complete the Site Configuration.
12. On the **Citrix** window, under **Site Setup**, verify the successful site creation. You can also click **Test Site configuration** to verify the site configuration.

Configuring the Virtual Delivery Agent software

To configure the Virtual Delivery Agent software:

1. Log in to the server.
2. Double-click the AutoSelect.exe file.

   The system displays a window with the following deployment option:

   - XenApp
   - XenDesktop

3. On the **XenApp Deliver applications** option, click **Start**.

   There are options for installing the following:

   - In the left pane, under **Get Started**, **Delivery Controller**. This option installs the Delivery Controller and other essential services like License Server and StoreFront. Citrix Delivery Controller for initial Citrix XenApp environment setup.
   - In the center pane, under Prepare Machines and Images:
     - Virtual Delivery Agent for Windows Server OS: This option is used to install agent to deliver applications and desktops from server-based VMs or physical machines.
     - Virtual Delivery Agent for Windows Desktop OS
   - In the right pane, under Extend Deployment the following options are available:
     - Citrix Director
     - Citrix License Server
     - Citrix StoreFront
     - Citrix Studio
     - Universal Print Server
4. On the **XenApp 7.5** window, in the center pane, click **Virtual Delivery Agent for Windows Server OS**.
5. In the **Environment** screen, in the **Configuration** section, under **I want to:** field, select **Enable connections to the server machine**.
6. Click **Next**.
7. In the **Core Components** screen, select **Citrix Receiver**.
8. Click **Next**.
9. **In the Delivery Controller** screen, in the **Configuration** section, under **Controller address** type the XenApp controller address.
10. Click **Test**.

    On successful verification of the controller address, a green tick mark appears next to the field.
11. Click **Next**.
12. In the **Features** screen, select the following:
    - Optimize performance
    - Use Windows Remote Assistance
    - Use Real-Time Audio Transport for Audio
13. Click **Next**.

14. On the **Firewall** screen, click Next.

    The system displays the Summary page. Review the prerequisites and confirm the components you want to install.

15. Click **Install**.
16. After successful installation, restart the server.

Note:
Repeat steps 1 to 16 on all the additional servers which are planned to be added to the Machine Catalog.

Creating machine catalog

To create machine catalog:

1. Log in to the server.
2. Open the Desktop Studio application.
3. On the **Welcome to Citrix Studio** screen, click **Set up machines for desktops and applications or remote PC access**.

   The system displays the **Machine Catalog Setup** window.

4. In the **Introduction** screen, click **Next**.
5. In the **Operating System** screen, select **Windows Server OS**.
6. Click **Next**.
7. In the **Machine Management** screen, select the following:
   - Under **This Machine Catalog will use** field, select **Machines that are not power managed (for example, physical machines)**.
   - Under **Deploy machines using** field, select **Another service or technology**.
8. Click **Next**.
9. In the **Machines** screen, click **Add Computers...**.
10. Select the Active Directory objects that you want to add.
11. Click **Next**.
12. In the **Summary** screen, under **Machine Catalog name** field, provide a name to the Machine Catalog.
13. Click **Finish**.

Configuring the Delivery group

Prerequisites

You must install Avaya Agent Rich Client before configuring the delivery group.

To configure Delivery group:

1. On the **Site Setup** screen, click **Set up Delivery Groups to assign desktops and applications to your servers**.

   The system displays the **Create Delivery Group** window.
2. In the **Getting started with Delivery Groups** screen, click **Next**.
3. In the **Machines** screen, select the required catalog and specify the number of machines for the delivery group.
4. Click **Next**.
5. In the **Delivery Type** screen, select one of the following options:
   - Desktops
   - Desktops and applications
   - Applications
6. Click **Next**.
7. In the **Users** screen, click **Add users...**.
8. Add the users from the Active Directory.
9. Click **Next**.
10. In the **StoreFront** screen, click **Next**.
11. In the **Applications** screen, you can add applications manually or change the application properties.
12. Click **Next**.
13. In the **Summary** screen, provide the following:
    - Delivery Group Name
    - Display name
    - Delivery Group description
14. Click **Finish**.
15. Click **Test delivery group**, to confirm that Delivery Group has been created successfully.

Displaying or modifying the application properties

To display or modify the application properties:

1. Open the **Citrix Studio** application.
2. In the left pane, select the **Delivery Groups** node.
3. In the **Action** pane, click **Properties**.
4. Display every option listed in the left pane to see or modify the configured settings.

   The system displays the **Application Settings** window.
5. In the **Identification** screen, set the following values under **Identify this application**.
   a. In the **Application name (for user)** field, type value as **Qui**.
   b. In the **Application name (for Administrators)** field, type value as **Qui**.
   c. In the **Description and keywords** field, provide a description for the application.
   d. Click **Apply**.
   e. Click **OK**.
6. In the **Delivery** screen, click **Application** icon and provide the icon.
7. Click **OK**.
8. In the **Location** screen, provide the following information:

Field	Value
Path to the executable file	%SystemDrive%\Avaya\IC73\bin\qui.exe
Command line argument (optional)	-d "C:\Avaya\IC73\apps\interaction_center" -n interaction_center
Working directory	%SystemDrive%\Avaya\IC73\bin

Note:

Create Avaya Agent INI `qui.ini` file in the path, `%SystemDrive%\Avaya\IC73\bin` with the below settings:

```
[QConsole]
ResizeDesktop=FALSE
```

9. Click **OK**.
10. In the **Limit Visibility** screen, you can set option to restrict access to the application.
11. Click **OK**.

12. In the **File Type Association** screen, click **OK**.

Creating a StoreFront

Prerequisite

Ensure that the StoreFront is installed.

To create a StoreFront:

1. Open the **Citrix StoreFront** console.
2. In the **Add StoreFront Server** window, provide the following:
   - StoreFront server name
   - Description
   - URL
3. Click **OK**.
4. In the **Citrix Studio** application, in the left pane, under the **Citrix StoreFront**, select the **Stores** node.
5. In the right **Action** pane, click **Manage Delivery Controllers**.
6. In the **Manage Delivery Controllers** window, click **Add...**.
7. In the **Edit Delivery Controller**, ensure that the correct type of server and protocol with port (HTTP or HTTPS) is selected.
8. Click **OK** to add the controller.
9. Install Citrix Receiver on Microsoft Windows 7 workstation.
10. To perform test login to StoreFront and connect to the application published in XenApp 7.5.
    a. Login to the Citrix StoreFront website.

       For example: *http://<IPAddress_CitrixServer>/Citrix/AARCWeb*
    b. In the left center, click the + (plus) sign.
    c. Click **All Apps** and verify the list of available applications.
    d. Click **Qui** to start the Avaya Agent Rich Client on Citrix.

Deploying Avaya Agent Rich Client on the Citrix server

To deploy the Avaya Agent Rich Client on the Citrix server:

1. Start the Citrix AppCenter Console.

2. In the left navigation pane, right-click the **XenApp** node under the **Citrix Resources** node and select **Create a new Citrix Farm**.

   The system creates a **NewFarmCitrix** node under the XenApp node.

3. In the left navigation pane, right click the Applications node under NewFarmCitrix and select **New** > **Publish application**.

   The system displays the Welcome page.

4. Click **Next**.

5. On the **Name** screen, enter the application display name and description and click **Next**.

   The system displays the Publish Application page.

6. On the **Type** screen, select the **Installed application** option and click **Next**.

   The system displays the Location page.

7. In the **Command line** field, enter the path of the `qui.exe` file.

   After you enter the `qui.exe` file path in the **Command line** field, the system displays the working directory of the `qui.exe` file in the **Working directory** field.

8. In the **Command line** field, modify the path of the `qui.exe` file as given below If the *`IC_INSTALL_DIR`*`\IC73\` resides on a C drive:

   ```
   C:\Avaya\bin\qui.exe" -d C:\Avaya\apps\interaction_center -n
   interaction_center
   ```

   Otherwise, select the appropriate drive and path.

9. Click **Next**.

10. Click **Add** at the bottom of the screen.

11. In the **Select Servers** window, select the Citrix server name and click **OK**.

12. On the **Servers** screen, click **Next**.

13. On the **Users** screen, select **Allow only configured users** option.

14. Click **Add** to add the configured users.

15. In the **Select Users or Groups** window, select the user name and click **Add.**

16. Click **OK** after you add all the required users.

17. On the **Users** screen, click **Next**.

18. On the **Shortcut presentation** screen, select the appropriate options and click **Next**.

19. On the **Publish immediately** screen, select the **Configure advanced application settings now** option and click **Next**.

20. On the **Access control** screen, select the appropriate option for the connection and click **Next**.

21. On the **Content Redirection** screen, click **Next**.

22. On the **Limits** screen, select the **Limit instances allowed to run in server farm** option and enter the appropriate value in the **Maximum instances** field.

    Note:
    If you want only one instance of application for each user, select the **Allow only one instance of application for each user** check box.

23. Click **Next**.
24. On the **Clients options** screen, click **Next**.
25. On the **Appearance** screen, select appropriate Session window size and Colors.
26. Click **Finish**.

Locating the files for the tools

The files for the tools are in the following directory on the IC Windows CD/DVD-ROM 1:

```
<CD/DVD-ROM_drive>\Utils\Citrix
```

Citrix XenDesktop

Citrix XenDesktop provides virtual Windows applications and desktops as secure mobile services. With XenDesktop, you can reduce costs by centralizing control and security of intellectual property. XenDesktop delivers full desktops or just the apps to remote device. XenDesktop is built on a 3rd generation FlexCast Management Architecture (FMA) and is the only hybrid cloud-ready platform that separates the management plane from the workload to enable IT to securely deliver published apps on-premises, and manage workers and mobile workspaces either on-premises or in the cloud.

For more information on Citrix XenDesktop see the Citrix website.

Note:
Avaya Agent Rich Client 7.3.3 is tested and supported with XenDesktop Virtual solution on Microsoft Windows 7 Operating System. You can login to XenDesktop using Citrix receiver client using the browser on the Desktop.

Installing the agent applications on the XenDesktop master image

You must perform the following procedure to run the Avaya Agent Rich Client on XenDesktop:

1. Install Avaya Rich Client application under C:\Program Files (x86) on XenDesktop master image of Windows 7 operating system. To install the agent desktop applications on a XenDesktop see Deploying Avaya Agent Rich Client on the Citrix server on page 429.
2. Give full access windows permissions to "C:\Program Files (x86)\Avaya\" directory for all AD domain users who are accessing XenDesktop remotely to use AARC.

Depending upon the environment, adjust the size of the Avaya Agent framework and then re-create the agent installer. For more information on customizing the framework size, see Avaya Agent Integration guide.

Configuring the Avaya Agent INI file

If the IC system includes agents accessing the Citrix client interface with the seamless window, you must configure the Avaya Agent INI file on each of the Citrix server or Citrix desktop/ application virtualization master image system that hosts IC agent desktop applications.

CAUTION:
Do not create or configure the Avaya Agent INI file on any system except a Citrix server that an agent will access through the Citrix client interface with the seamless window. The parameter needed for the seamless window can cause undesirable formatting and sizing of the Avaya Agent in other deployments.

To configure the Avaya Agent INI file:

1. In Notepad or another text editor, open a new document.
2. Type the following information into the document:

```
[QConsole]
ResizeDesktop=FALSE
```

3. Save the file with the following name: `qui.ini`
4. Install the file in the Windows installation directory on each Citrix server that hosts IC agent desktop applications.

   For example, the Windows installation directory is typically either `C:\Winnt` or `C:\Windows`.
5. If qui.ini file already exist user can just edit the file and append above step 2 parameters and save the file.

Configuring the Web Client URL pre-requisite on Citrix XenDesktop Master Image

Avaya IC 7.3.3 and later versions, supports access to web client for the agents who are logged in through Citrix XenDesktop solution.

The following procedure provides details on how to login to thin client agent on all published Citrix XenDesktops.

To configure web client URL pre-requisite on Citrix XenDesktop master image before publishing for XenDesktop creation, do the following:

1. XenDesktop master image must have the supported version of Internet explorer.
2. Ensure that the latest JRE 8, 32 bit is installed on master image and the Internet Explorer browser is using JRE 8 to login to Avaya Agent Web Client.
3. Launch the Internet Explorer.
4. Access Avaya Agent Web Client URL.

   http://<WebConnectorServerIP>:<TomcatPort>/avaya/agent
5. Accept and install Active X Control installation options, if any.
6. Choose to allow access to all required controls.
7. Verify if IC agent is logged in successfully on the thin client.
8. Logout of Avaya Agent Web Client.

Note:

Avaya Agent Web Client is tested and supported with XenDesktop Virtual solution on Internet Explorer 10 and 11 of Microsoft Windows 7 Operating System. You can login to XenDesktop from the browser of your desktop using Citrix receiver client.

Configuring the IC Web browser tool

To use the IC Web browser tool to access the agent desktop applications on the Citrix server:

1. Configure the IC Web browser tool.
2. Copy the files to the system that hosts the Web server used by IC.

This section includes the following topics:

- Components of the Web browser tool on page 434
- Installing the Web browser tool on page 434
- Updating the HTML page for the Web browser tool on page 435
- Accessing more than one Citrix server on page 436

Components of the Web browser tool

The IC Web browser tool includes the files listed in the following table.

File	Description
ActiveX control	SetupLocalDesktopForAgentViaCitrixCtr.CAB Digitally signed ActiveX control with unique class ID
HTML access page	`BasicStartAgent.htm` • Specifies the URL for the applications on the Citrix server. • Determines the text that the agent sees on the links. You can customize this text.

Installing the Web browser tool

To install the Web browser tool:

1. For Avaya IC systems that use Microsoft IIS as the Web server, when you set up and test the Web browser tool, configure a virtual directory in IIS for the Web browser tool.
2. Copy the following files to the system that hosts the Web server used by the IC system:
   - `SetupLocalDesktopForAgentViaCitrixCtr.CAB`
   - `BasicStartAgent.htm`

   For example, if the IC system uses the Microsoft IIS as the Web server, copy the files to the system that hosts that Web server.

Updating the HTML page for the Web browser tool

The following table describes the parameters you can configure and add to the HTML page. The only required parameter is CitrixClientURL.

CAUTION:
Do not delete or change the javascript or other code in the HTML page.

Property	Description
CitrixClientURL	Specifies the location of the startup link for the IC agent desktop applications on the Citrix server. The value for the property must be a valid URL. For example: `CitrixClientURL="http://`*server_name.com*`/ICAgent/ICAgentAppMode.ica"`
<A href="javascript: Main.SetDesktopForICAgent() "> Start Avaya Agent</A>	Specifies the text on the link that the agent clicks to access the agent desktop applications on the Citrix server.
<A href="javascript: Main.ResetDesktop();window. close()">EXIT</A>	Specifies the text on the link that the agent clicks to close the interface with the agent desktop applications on the Citrix server.
<A href="javascript: Main.ForcedResetDesktop()"> Force Reset</A>	Specifies the text on the link that the agent clicks to force a reset of the interface with the agent desktop applications on the Citrix server in the event of a failure.
DontStartMultipleInstancesOf Agent	Determines how the tool acts when an agents logs in to and exits from the tool. This property is optional. You can add it to the HTML page, if required. For more information, see DontStartMultipleInstancesOfAgent on page 438.

In addition to the parameters in the above table, you can also customize the HTML page as follows:

- Add a corporate logo, a graphic for the background, or otherwise customize the appearance of the HTML page.
- Add one or more of the properties in the Application or Desktop sections of the INI file for the executable tool, as described in Updating the INI file for the IC executable tool on page 437.

Note:
You cannot add properties from the GUI section of the INI file for the executable tool.

Accessing more than one Citrix server

If the agents need to access the agent desktop applications on more than one Citrix server:

1. For each Citrix server that hosts agent desktop applications, configure the files for a Web browser tool.
2. Install the following files in the same folder on the system that hosts the Web server:
   - One copy of the ActiveX control: `SetupLocalDesktopForAgentViaCitrixCtr.CAB`
   - For each Citrix server that the agents need to access, one copy of `BasicStartAgent.htm`
3. Create a desktop icon or an Internet Explorer **Favorites** menu for each Web browser tool.

Configuring the executable tool

To use the IC executable tool to access the agent desktop applications on the Citrix server:

1. Configure the IC executable tool.
2. Copy the files to either the agent workstations or to a network share that can be accessed by all agents.

This section includes the following topics:

- Components of the executable tool on page 437
- Installing the executable tool on page 437
- Updating the INI file for the IC executable tool on page 437
- Accessing more than one Citrix server on page 440

Components of the executable tool

The IC executable tool includes the files listed in the following table.

File	Description
Executable file	`SetupLocalDesktopForAgentViaCitrix.exe` Launches the dialog box used by agents to access the Citrix server that hosts the agent desktop applications.
INI file	`AgentDesktopCtr.ini` After you update this file: • Specifies the directory path to the agent desktop applications on the Citrix server. • Determines the text on the buttons in the dialog box. You can customize this text to suit the needs of the contact center and to match the corporate style.

Installing the executable tool

You can install the executable in either of the following locations:

- On a network share that is accessible to all agents who need to use the executable tool.
- Every agent workstation used by an agent who needs to use the executable tool.

To install the executable tool, copy the following files to the required location:

- `SetupLocalDesktopForAgentViaCitrix.exe`
- `AgentDesktopCtr.ini`

Updating the INI file for the IC executable tool

The following table describes the parameters that you can configure and update in the **AgentDesktopCtr.ini file**. The only required parameter is the directory path for the agent desktop applications on the Citrix server.

Section	Property	Description
APPLICATION	CitrixClientURL	Specifies the location of the startup link for the IC agent desktop applications on the Citrix server. The value for the property must be a valid URL. For example: `CitrixClientURL="http://`*server_name.com*`/ICAgent/ICAgentAppMode.ica"`

Section	Property	Description
APPLICATION	DontStartMultipleInstancesOfAgent	Determines how the tool acts when an agents logs in to and exits from the tool. Default setting is TRUE. When this property is set to TRUE, if an agent logs out of Avaya Agent without exiting from the tool, the agent cannot use the tool to log back in to Avaya Agent. Instead, the agent sees an error which states that Avaya Agent is already running. The agent must follow the correct sequence of steps if you use this setting. For more information, see Sequence for using the Avaya tools for Citrix on page 440. When this property is set to FALSE, if an agent logs out of Avaya Agent without exiting from the tool, the agent can use the tool to log back in to Avaya Agent. The tools will allow the agent to start a "new" instance of Avaya Agent.
APPLICATION	AgentAlreadyRunningMsg	Specifies the message displayed to the agent if an interface is already open and you set DontStartMultipleInstancesOfAgent is set to TRUE. For example, `AgentAlreadyRunningMsg=The Avaya agent was already started`
DESKTOP	ClientBarHeight	Controls the desktop area reserved for the bottom of the Avaya Agent framework. The default value is 125 pixels. For example, `ClientBarHight= 151`
DESKTOP	ClientBarWidth	Controls the desktop area reserved for the left side bar of the Avaya Agent framework. The default value is 200 pixels. For example, `ClientBarWidth=201`

Section	Property	Description
GUI	Caption properties	The following caption properties allow you to specify the text for the dialog box: • `WindowCaption="Avaya Agent Desktop Control (customize me)"` • `StopButtonCaption="Exit Avaya Agent (customize me)"` • `StartButtonCaption="Start Avaya Agent (customize me)"` • `ResetButtonCaption="Reset Desktop (customize me)"` • `ApplicationFrameCaption="Application Controls (customize me)"` • `ResetFrameCaption="Emergency Control (customize me)"`
GUI	MinimizeWindowOnLanchedAppStart	Automatically minimizes the interface after the agent accesses the agent desktop applications on the Citrix server. For example, `MinimizeWindowOnLanchedAppStart=TRUE`
GUI	MaximizeWindowOnLanchedAppExit	Automatically maximizes the interface after the agents starts the agent desktop applications on the Citrix server. Only set this property to TRUE if you also set AutoResetOnExit to TRUE. For example, `MaximizeWindowOnLanchedAppExit=TRUE`
GUI	DisableStartButtonAfterFirstClick	Automatically disables the **Start** button on the dialog box after the agent starts the agent desktop applications on the Citrix server. For example, `DisableStartButtonAfterFirstClick=FALSE`
GUI	AskForExitConformation	Ensures that the interface asks the agent to confirm before exiting the interface to the Citrix server. Set this property to FALSE if you experience problems with minimizing or maximizing Avaya Agent. For example, `AskForExitConformation=FALSE`

Accessing more than one Citrix server

If an agent needs to access the agent desktop applications on more than one Citrix server:

1. For each Citrix server that hosts agent desktop applications, configure the files for a executable tool.
2. Install a executable tool for each Citrix server in separate folders on the agent workstation.
3. Create a desktop icon or **Start** menu item for each executable tool.

Sequence for using the Avaya tools for Citrix

Agents must use the following sequence when they use either the Web browser tool or the Executable tool. If an agent does not follow this sequence, Avaya Agent and other agent desktop applications may no longer size properly in the Citrix interface.

The proper sequence for using the Avaya tools for Citrix is:

1. Agent starts the Avaya tool:
   - For Web browser tool, agent clicks the **Start** link.
   - For the Executable tool, agent selects **Start**.

   Avaya Agent on the Citrix server starts.
2. Agent logs in to Avaya Agent through Citrix.
3. Agent handles contacts and performs required tasks in Avaya Agent.
4. Agent logs out from Avaya Agent through Citrix.
5. Agent exits the Avaya tool:
   - For Web browser tool, agent clicks the **Exit** link.
   - For Executable tool, agent selects **Exit**.
6. On the **Citrix AppCenter** console, verify that the Rich Client application is successfully added under the **Citrix applications** node.

   You can change the published application setting from the Citrix AppCenter console.
7. Modify the Avaya Agent INI file:
   a. Update the Citrix server's qui.ini file with the following two lines:

      ```
      [QConsole]
      ResizeDesktop=FALSE
      ```

   b. Save the qui.ini file.

Creating ICA (Citrix Client) connection with Citrix server

To create an ICA (Citrix Client) connection with Citrix server:

There are two ways to install Citrix client. They are:

- Method A: Using Citrix Program Neighborhood on page 441
- Method B: Using Citrix ICA Quick Launch Tool on page 442

Method A: Using Citrix Program Neighborhood

To use Citrix Program Neighborhood:

1. Install Citrix Program Neighborhood on the Windows XP/Windows 7 system.
2. On the Citrix client system, open Citrix Program Neighborhood.
3. Add a new ICA connection.
4. Select Local Area Network and click **Next**.

   The system displays the Add New ICA Connection window.
5. Enter the description for the new ICA connection.
6. Select the network protocol.
7. Select the **Published Application** option and click the drop-down list to select the published application that you want to connect.

   Note:
   If you select the **Server** option, the system remotely connects with the Citrix server using Remote Desktop Connection (RDC).
8. Click **Server Location**.

   The system displays the Locate Server or Published Application window.
9. Click Add to add the Citrix server name in the **Address List** field.
10. Click **OK**.
11. On the Add New ICA Connection page, click **Next**.
12. Select published view option and click **Next**.
13. Select the appropriate option.
14. Select the encryption level and click **Next** (Use default).
15. Enter the login credential of the Citrix server.

    Note:
    You must have the access permission of the published application from the Citrix XenApp.

16. Select the display options and click **Next**.
17. Click **Finish**.
18. In the Citrix Program Neighborhood window, ensure that the Citrix Client connection is successfully added.
19. Double-click the added Citrix Client connection.

    It will start session from the server side, and you can then access the published applications.

Method B: Using Citrix ICA Quick Launch Tool

To use Citrix ICA Quick Launch Tool:

1. Install the Citrix ICA Client and Citrix QuickLaunch Tool on Windows XP or Windows 7 system.
2. Open the Citrix QuickLaunch Tool from Citrix client system.
3. In the **Citrix QuickLaunch Tool** window, click **Options>>**.
4. Under **Please specify the server or farm information** field, add the XenApp Server address and XML Service Port number. This is the port number that was specified while configuring PNAgent.
5. Under **Select the type of ICA connection** field, select **to a Published App** option and select the Published application from the list.
6. Under **ICA Options** field, in the **Encryption Level** field, select the required encryption level.
7. Under **Credentials** field, provide the login credentials of the Citrix XenApp server.

   Note:

   The login credential used to login to Citrix XenApp server must have permission of published application from Citrix presentation server.
8. Click **Write ICA File** and provide the path to save the ICA file.
9. Double-click the saved ICA file or click **Connect** in the **Citrix QuickLaunch Tool** window to start Avaya agent.

Chapter 15: Installing Avaya Agent Web Client

Avaya Agent Web Client is a Web based component of Avaya Interaction Center (IC) application. Using Avaya Agent Web Client, you can contact customer on the Web. You can chat with customer, collaborate the chat session with multiple agents, or even involve additional people referred by the customer.

Installation of Avaya Agent Web Client includes installation of **WebClient** and installation of **Web Client Connector**.

WebClient installation generates a web-application WAR file that contains all the required WebClient components, JAR files, and so on. You must install WebClient only on Windows system.

After you generate the web-application WAR file, it needs to be deployed on the Web Client Connector system. You can install Web Client Connector on all the Avaya supported platforms.

When you install Avaya Agent Web Client in a contact center:

- Do not install Avaya Agent Web Client on an agent workstation.

  Important:
  Read the IC Readme file and *Avaya IC Installation Planning and Prerequisites* before you install and deploy Avaya Agent Web Client.

For information about how to customize Avaya Agent Web Client, see *Avaya Agent Web Client Customization*.

This section includes the following topics:

1. Prerequisites for Avaya Agent Web Client on page 445
2. Installing the Avaya Agent Web Client on page 447
3. Creating the application WAR file on page 449
4. Setting up the Java Application Bridge on page 449
5. Installing the Avaya Agent Web Client Connector on page 456
6. Re-installing Avaya Agent Web Client connector on page 458

Prerequisites for Avaya Agent Web Client

This section includes information that you need to know and steps you must perform before you install and deploy Avaya Agent Web Client. Ensure that you have completed the prerequisites described in the following topics.

- IC components on page 445
- Agent workstations on page 445
- JRE version on page 446
- Required administrator privileges on page 446
- Working directory property on page 447
- Internet connectivity on page 447

IC components

For IC components, ensure that you have completed the following tasks:

- Install and configure all IC prerequisites, as described in *Avaya IC Installation Planning and Prerequisites*.
- Install and configure Avaya IC, including all media channels.
- Configure agents for Avaya Agent Web Client, as described in Configuring the working directory property on page 390.

Agent workstations

Install and configure the following prerequisites on all agent workstations that are used to access Avaya Agent Web Client:

- Install Internet Explorer with the Oracle Java Plug-in enabled. By default, Microsoft Internet Explorer uses the Microsoft Java Plug-in.
- Configure the internet options of Internet Explorer as follows:
  - Security level: Medium if agents uses Windows Server 2008 R2.
  - ActiveX controls: allow to run.

    Add the URL of the Avaya Agent Web Client system to the Trusted Sites list.

- Proxy server settings: Add the fully qualified domain name of the contact center to the proxy **Exceptions** field. For example, you can enter ***.company_name.com** or ***.*.company_name.com**. You can add multiple names. Check the documentation for your operating system for details.
- Pop-up blockers: disable or configure to allow pop-ups on the Avaya Agent Web Client URL.

JRE version

Avaya Agent Web Client requires the following versions of JRE:

Web Client Connector systems: The installer for Web Client Connector automatically installs the required version of JRE. The JRE version installed by this installer remains independent of the JRE version you already have on a system.

Avaya Agent Web Client on agent desktop systems: Requires at least JRE version 1.6.0_45. Avaya Agent Web Client automatically installs the required version if JRE is not installed. If an older version of JRE is already installed, you must upgrade JRE to the latest version.

Required administrator privileges

The installer for Avaya Agent Web Client requires the same administrator privileges as the installers for the IC servers and the IC Design & Administration Tools. For more information, see Required administrator privileges on page 29.

Important:
You can install Avaya Agent Web Client as root or as a user with the same privileges as root. If you install as root, do not run Avaya Agent Web Client as the root user.

For more information on ownership on Solaris, see Changing ownership for Avaya Agent Web Client on Solaris only on page 463.

For more information on ownership on AIX, see Changing ownership for Avaya Agent Web Client on AIX only on page 463.

Working directory property

The working directory holds Avaya Agent Web Client agent settings for agents, agent resources, and global resources. Avaya Agent Web Client uses agent file persistence to save settings for each agent.

CAUTION:
If you do not use a valid directory path when you configure the working directory, Avaya Agent Web Client does not function properly. Avaya Agent Web Client displays an error message on the status bar, and the chat and email channels are disabled.

For more information about the working directory and recommended settings for that directory, see Configuring the working directory property on page 390.

Internet connectivity

The agent machine running AAWC requires Internet connectivity.

For enhanced security, Oracle has introduced a feature to check the certificate revocation. Before Java attempts to launch a signed application, the associated certificate is validated to ensure that it has not been revoked by the issuing authority. This feature makes Internet access mandatory for agent machines running AAWC.

Note:
You can manually disable the revocation check from the Java Control Panel. However, it is not recommended and the action might raise security concerns.

Installing the Avaya Agent Web Client

Avaya Interaction Center, Release 7.3.x provides the `icclientsuite` installer that you can run to install Avaya Agent Web Client. You can download the `icclientsuite` installer using the `install.htm` file and other required files provided in Avaya Interaction Center, Release 7.3.x.

To download the installer:

1. Double click the `install.html` file.

   The Internet Explorer window opens with the **Welcome** page and a button for downloading the installer.

2. Click the **Download Installer for Windows** button.

   The **File Download** dialog box opens with options for running or saving the installer.

3. Click **Run** to run the installer from the server.

   OR

4. Click **Save** to first save the installer on your local system and then run it.

To install Avaya Agent Web Client on Windows systems:

1. Go to the location where you have downloaded the `iclientsuite` installer, the `install.exe` file.
2. Double click the `install.exe` file.

   The InstallAnywhere launch the `icclientsuite` installer with **Introduction** page.

3. Click **Next** to continue.

   The **License Agreement** page displays.

   Note:
   Read the license information carefully.

4. Select **I accept the terms of the License Agreement** to accept the license and click **Next** to continue.

   The **Component Selection** page displays.

5. Select **AAWC** and click **Next**.

   The **Choose Install Folder** page displays.

6. Enter or choose the location where you want to install the Avaya Agent Web Client.

   Note:
   Keep the default location for installing Web Client.

7. Click **Next**.

   The system displays the **Pre-Installation Summary** page. You can see the summary of the options that you have selected in the earlier steps. This page also displays the available space and the space that is required for installing the Web Client.

   Note:
   Check the summary carefully. If you want to change any information, click the **Previous** button to go to the previous page.

8. Click **Install**.

   The Avaya Agent Web Client installation starts. After the Web Client is installed successfully, the system displays the **Install Complete** page. The page displays the folder location where the Web Client is installed successfully.

9. Click **Done**.

Creating the application WAR file

To create the WAR file:

1. Go to the location where you have installed the Avaya Agent Web Client.

   Note:
   The default location is *IC_INSTALL_DIR*\IC73\Avaya IC Client Suite 7.3

2. Double click the `wargenerater.bat` file.

   The Command Prompt console opens. After completing the process, the `webclient.war` file is created in the folder where Avaya Agent Web Client is installed.

   Note:
   If you are migrating from Avaya IC 7.1 to Avaya IC 7.3, first you need to manually merge all your customization scripts, JSP scripts, and properties and then generate the WAR file.

Setting up the Java Application Bridge

The Application server for Avaya Agent Web Client uses the Java Application Bridge to communicate with the IC servers and databases.

This section includes the following topics:

- Configuring an agent account for the Java Application Bridge on page 449
- Creating a Java Application Bridge on page 451
- Setting up UNC to UNIX mapping on page 454
- Setting up UNC to UNIX mapping on page 454

Configuring an agent account for the Java Application Bridge

The Java Application Bridge requires a non-human agent account for IC. This account is the DCO Bridge account.

The IC seed data includes one non-human agent account for the DCO Bridge. You can use this account for the first Java Application Bridge in the IC system.

You must create a unique non-human agent account for each additional Java Application Bridge in the IC system. Name each account dcobridge*N*. The agent name can also include the name of the system that hosts the Java Application Bridge.

Tip:
The following instructions describe how to create additional non-human agent accounts for the Java Application Bridge. If you use the account in the IC seed data, you should double-click that agent account and complete step 5 below.

To configure an agent account for the Java Application Bridge:

1. In IC Manager, click the **Agent** tab.
2. In the left pane, expand the **DefaultTenant** node.

   If you want to create this agent account in a different tenant, expand that node in the left pane instead of **DefaultTenant**.
3. Select **Agent** > **New**.
4. On the **General** tab enter the information for the fields as described in the following table:

Field	Recommended entry
First Name	dcobridge*N* (for example, dcobridge2)
Last Name	dcobridge*N* (for example, dcobridge2)
Preferred Name	dcobridge*N* (for example, dcobridge2)
Employee ID	dcobridge*N* (for example, dcobridge2)
Login ID	dcobridge*N* (for example, dcobridge2)
Domain	The same user domain as the Java Application Bridge that uses this agent account. For example, User1.
Task Load	0
Task Ceiling	0
Site	DefaultSite

5. Click the **Security** tab and enter the information for the fields as described in the following table:

Field	Recommended entry
Password	Enter a password for this account. **Tip:** Change the password for the pre-defined Java Application Bridge account.
Confirm	Re-enter the password for this account.

Field	Recommended entry
Force password change on login	Clear this field. Do not select this field for non-human IC users
Disable login	Do not select this field.
Role	Select the **Agent** role. **Note:** Do not select any of the other roles.

6. Click **Ok**.

Creating a Java Application Bridge

The Java Application Bridge is not a true IC server. The Java Application Bridge impersonates each agent who logs in to the Avaya Agent Web Client. When the Java Application Bridge makes a request for an agent, the Java Application Bridge mirrors the domain structure of the agent.

You must create a Java application bridge for each Avaya Agent Web Client application.

To configure a Java application bridge:

1. In IC Manager, click the **Server** tab.
2. Select **Server** > **New**.
3. From the list of servers, select **JavaAppBridge**.
4. Click **Ok**.

5. On the **General** tab enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
Name	Enter a name for the Java Application Bridge.	Include the name of the system that hosts the Web Client Connector application server to identify the location of the JavaAppBridge.
Domain	Select an IC User domain for the Java Application Bridge from the drop-down list.	For example, select `User1` from the drop-down list. Assign the Java Application Bridge to the same User domain as the majority of the agents who use Avaya Agent Web Client. If the IC system includes Avaya Agent Web Client at different sites, use the User domain that contains the majority of agents at that site. If the IC system includes agents in multiple domains, you do not need a Java Application Bridge in each User domain. Ensure that the domain with the Java Application Bridge fails over to the following domains: • Itself • The Default domain • All domains with an ADU server
Host	Enter the IP address of the system that hosts Web Connector.	
Port	Enter a port assignment for the Java Application Bridge.	You can use any available port in the 9000 range for the Java Application Bridge. If you do not host other IC servers on the same system as Web Client Connector, use port 9002.

Field	Recommended entry	Notes
Directory	Enter the path to the `etc` directory for Avaya Agent Web Client.	For example enter: *`IC_INSTALL_DIR`*`\IC73\etc` where *`IC_INSTALL_DIR`* is the path to this directory on the Web Connector system. For example, if you used the default, the path would be: `C:\Avaya\IC73\etc`
Executable	Enter `jabsrv`	Leave the default entry. **Tip:** This entry exists because this is a required field in IC Manager. No separate executable exists.

6. Record the **Name** value for the Java Application Bridge.
7. Click the **JavaAppBridge** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Notes
IC User	Enter the name of the agent account for this Java Application Bridge server.	Use the agent account that you created in Configuring an agent account for the Java Application Bridge on page 449. For example, enter dcobridge1.
IC Password	Enter the password associated with the agent account.	

8. Click **Ok**.

   Do not start the Java Application Bridge.

   You can start the Java Application Bridge:

   - By running the `aawcclient.bat` script
   - By running `aawcclient.sh` script
   - By running `aawcclient.sh` script

Setting up UNC to UNIX mapping

The **UNC to UNIX Path Mapping** field of the Java Application Bridge maps the UNC address of a network folder which holds files that agents can attach to resources with the UNIX path that Web Client Connector uses to access the folder.

Tip:
You do not need to map the working directory for the Web Client Connector system. However, you can map this directory if required.

This section includes the following topics:

- Prerequisites for UNC to UNIX path mapping on page 454
- Requirements for entries in the UNC to UNIX Path Mapping field on page 454
- Accessing multiple folders on a system on page 455
- Examples of entries in the UNC to UNIX Path Mapping field on page 455
- Configuring UNC to UNIX Path Mapping on page 456

Prerequisites for UNC to UNIX path mapping

You must perform the following steps before you configure UNC to UNIX path mapping:

1. Install Samba (or an equivalent product) on the UNIX system that hosts the attachments directory to make the folders and files accessible from a Windows system.
2. Configure the UNIX shares for Samba (or an equivalent product) as follows:
   a. Ensure that the name of each share is the same as the UNIX folder that it shares.
   b. Ensure that all agents have Read permissions for the share. You can give the agents additional permissions for the share, if required.
   c. Ensure that the UNIX user under which Avaya Agent Web Client runs has the same permissions for the UNIX directory as agents have for that directory's share.

Requirements for entries in the UNC to UNIX Path Mapping field

Follow these requirements when you enter information in the **UNC to UNIX Path Mapping** field:

- You can only create one entry for each system. The Java Application Bridge only considers the first entry for a given system in the table. All subsequent entries are ignored.
- You can only use the format ***system_name*** in the **UNC System Name** column.
- You can only use valid UNIX paths in the **UNIX Path** column.

Accessing multiple folders on a system

You cannot add multiple entries for a system in the **UNC to UNIX Path Mapping** field.

If you want to store files for attachments in multiple folders on the same system:

1. Organize the folders so that they are all subfolders of a single folder. For example, create an attachments folder with subfolders titled printers, ink, and cables.
2. Use Samba (or an equivalent product to configure the UNIX shares named printers, ink, and cables for the subfolders of the attachments folder.
3. Give agents Read permissions, at a minimum, for the shares.
4. In the **UNC System Name** column, enter the name of the system where the attachments folder is located. For example, **`\\sunbox1`**.
5. In the **UNIX Path** column, enter the UNIX path for the **`attachments`** directory. For example, **`/opt/attachments`**.

Examples of entries in the UNC to UNIX Path Mapping field

The following table shows a series of entries in the **UNC to UNIX Path Mapping** field, including both valid and invalid entries.

UNC to UNIX Path Mapping entry		**Description**
UNC System Name	**UNIX Path**	
\\sunbox1	/opt/data/attachments	A valid entry in both columns.
\\sunbox2\	/opt/data/attachments	An invalid entry in the **UNC System Name** column. The Java Application Bridge cannot accept an entry that ends with a backslash.
\\sunbox1	/opt/data	Entry is ignored as there is already an entry for this UNC system name.
\\sunbox3	/	A valid entry in both columns. The **UNIX Path** entry points to the root directory on the system.
\\sunbox4		An invalid entry in the UNIX Path column. For root directory, enter /, as shown in the above entry.

Configuring UNC to UNIX Path Mapping

The **UNC to UNIX Path Mapping** field of the Java Application Bridge maps the UNC address of a network folder which holds files that agents can attach to resources with the UNIX path that Web Client Connector uses to access the folder.

Alarms are generated and added to the logs if an error is detected. For more information, see Troubleshooting the Java Application Bridge in the *Troubleshooting Interaction Center Guide*.

To configure UNC to UNIX path mapping for Web Client Connector:

1. If necessary, double-click the Java Application Bridge in the **Server** tab of IC Manager.
2. Click the **JavaAppBridge** tab.
3. Click the Ellipsis (**…**) button next to the **UNC to UNIX Path Mapping** field.
4. In the **UNC to UNIX Path Mapping** dialog box:
   a. Click **New**.
   b. In the **UNC System Name** column, enter the name of the system that hosts the attachments folder in UNC format. For example, enter **`\\testbox`**
   c. In the **UNIX Path** column, enter the path that the Web Client Connector system uses to access the attachments folder. For example, enter **`/opt/data/attachments`**
   d. After you create entries for each attachments folder, click **Ok**.
   e. Click **Ok** to close the Server Editor.
   f. Restart the Avaya Agent Web Client application server in the Web Client Connector system.

Installing the Avaya Agent Web Client Connector

Avaya Interaction Center, 7.3 provides the `icserversuite` installer that you can run to install Web Client Connector. You can download the `icserversuite` installer using the `install.exe` install.bin file and other required files provided in Avaya Interaction Center, Release 7.3.x.

To install Web Client Connector:

1. Go to the location where you have downloaded the `install.exe` install.bin file.
2. Double click the `install.exe` file.

   The InstallAnywhere launch the `icserversuite` installer with **Introduction** page.
3. Click **Next** to continue.

   The **License Agreement** page displays.

Note:
Read the license information carefully.

4. Select **I accept the terms of the License Agreement** to accept the license and click **Next** to continue.

   The **Component Selection** page displays.

5. Click **WebConnector** and click **Next**.

   The **Choose Install Folder** page displays.

6. Enter or select the location where you want to install the Web Client Connector.

Note:
Keep the default location for installing Web Client Connector.

7. Click **Next**.
8. The **Choose Shortcut Folder** page is displayed.
9. Select any one location where you want to create a shortcut for running the Web Client.

Note:
For some of the options, you can select the **Create Icons for All Users** check box to create the shortcuts for all the users.

10. Click **Next**.

    The **Pre-Installation Summary** page is displayed. You can see the summary of the options that you have selected in the earlier steps. This page also displays the available space and the space that is required for installing the Web Client.

Note:
Check the summary carefully. If you want to change any information, click the **Previous** button to go to the previous page.

11. Click **Install**.

    The Web Connector installation starts. After the Web Connector is installed successfully, the **Install Complete** page is displayed. The page displays the folder location where the Web Connector is installed successfully.

12. Select **Run Configuration tool**. For more information, see Running the configuration tool on page 461.
13. Click **Next**.
14. Select **Client** mode.
15. Click **Next**.
16. Click **Done**.

    After successful installation of Web Client on the Windows platform, you can configure the Avaya Agent Web Client. For more information, see Configuring Avaya Agent Web Client on page 460.

Re-installing Avaya Agent Web Client connector

If you need to re-install the Avaya Agent Web Client connector, you must first remove the existing Avaya Agent Web Client connector. For more information, see Uninstalling Avaya Agent Web Client in the *Troubleshooting Interaction Center Guide*.

Chapter 16: Configuring and Deploying Avaya Agent Web Client

Avaya Agent Web Client is a Web based component of the Avaya Interaction Center (IC) application. After you successfully install the Avaya Agent Web Client, you must configure and deploy it on a system where Web Client Connector is installed. This chapter explains all the procedures that helps you configure and deploy Avaya Agent Web Client.

Important:
Read the IC Readme file and *Avaya IC Installation Planning and Prerequisites* before you install and deploy Avaya Agent Web Client.

For information about how to customize Avaya Agent Web Client, see *Avaya Agent Web Client Customization*.

This section includes the following topics:

1. Before you configure and deploy Avaya Agent Web Client on page 460
2. Configuring Avaya Agent Web Client on page 460
3. Verifying the deployment of AAWC on page 468
4. Redeploying the application WAR file on page 468

Before you configure and deploy Avaya Agent Web Client

Before you start configuring and deploying the Avaya Agent Web Client, ensure that you have successfully created the application WAR file. For more information, see Creating the application WAR file on page 449.

This section explains about the basic and advance options available for configuring Avaya Agent Web Client.

Configuring Avaya Agent Web Client

- Basic Configuration on page 461
- Advance Configuration on page 466

Basic Configuration

This section includes the following topics:

- Running the configuration tool on page 461
- Deploying the application WAR file on page 462
- Changing ownership for Avaya Agent Web Client on Solaris only on page 463
- Changing ownership for Avaya Agent Web Client on AIX only on page 463
- Starting and stopping Avaya Agent Web Client on page 463
- Setting the options in Internet Explorer 9.0 and later on page 464
- Testing Avaya Agent Web Client on page 466

Running the configuration tool

Important:
Before running the configuration tool, ensure that you have added the FQDN of all the IC systems to host file of each IC system.

To run the configuration tool:

1. Start the Configuration Tool:

Operating system	Procedure
Windows	Select **Start** > **Programs** > **Avaya Interaction Center 7.3** > **Configuration Tool**.
Solaris	1. Navigate to *IC_INSTALL_DIR*/IC73/bin 2. Run **./configure**
AIX	1. Navigate to *IC_INSTALL_DIR*/IC73/bin 2. Run **./configure**

2. On the **Initial Configuration** page of the Configuration Tool, select **Client** as the configuration mode.
3. Enter the primary host name.

Note:
Ensure that the system that you have specified as the primary host is reachable from the system on which you are running the Configuration Tool. If required, you must add the FQDN of a system specified as the primary host to the host file.

4. Keep the default settings for other options, and click **Apply Settings**.

   The `vesp.imp` file is copied on a Web Client Connector System.

Deploying the application WAR file

To deploy the application WAR file:

1. Copy the `webclient.war` file, which is generated during the installation of AAWC installation. For more information, see Creating the application WAR file on page 449.
2. Paste the `webclient.war` file in the *IC_INSTALL_DIR*`/IC73/tomcat/Avaya/war` directory, on the Web Client Connector system.
3. From the webconnector system, run the Configuration Tool as mentioned in the below table:

Operating system	Procedure
Windows	Select **Start** > **Programs** > **Avaya Interaction Center 7.3** > **Configuration Tool**.
Solaris	1. Navigate to *IC_INSTALL_DIR*`/IC73/bin` 2. Run **`./configure`**
AIX	1. Navigate to *IC_INSTALL_DIR*`/IC73/bin` 2. Run **`./configure`**

4. Enter the user name and password for administrator.
5. Click **Ok**.
6. Click the **Web Client** tab and specify the Web Client URL: `http://<IP_of_system_on_which_WebConnector_is_installed>`
7. Specify the Java Application Bridge Name. For information, see Creating a Java Application Bridge on page 451.
8. Click **Apply Settings**.

   The message box is displayed with a message that the settings are applied successfully.
9. Click **Ok**.
10. Click **Exit**.

Changing ownership for Avaya Agent Web Client on Solaris only

If you installed Avaya Agent Web Client as the root user, change ownership for Avaya Agent Web Client to run under a non-root user.

Important:
Users must avoid running IC software as the root user wherever possible for security reasons. Create a user for the IC system before you perform these steps. For more information, see *Avaya IC Installation Planning and Prerequisites*.

Changing ownership for Avaya Agent Web Client on AIX only

If you installed Avaya Agent Web Client as the root user, change ownership for Avaya Agent Web Client to run under a non-root user.

Important:
Users must avoid running IC software as the root user wherever possible for security reasons. Create a user for the IC system before you perform these steps. For more information, see *Avaya IC Installation Planning and Prerequisites*.

Starting and stopping Avaya Agent Web Client

In the Avaya Interaction Center, Release 7.3.x, you can start and stop the Avaya Agent Web Client component by handling the `javaw` process.

To start or stop the javaw process:

1. Open the command prompt by selecting **Start** > **Run**.
2. Change the directory to: *`IC_INSTALL_DIR`*`\IC73\bin`.
3. Execute the following command:

Operating system	Procedure
Windows	To start: `aawcclient.bat start` To stop: `aawcclient.bat stop`
Solaris	To start: `./aawcclient.sh start` To stop: `./aawcclient.sh stop`
AIX	To start: `./aawcclient.sh start` To stop: `./aawcclient.sh stop`

Setting the options in Internet Explorer 9.0 and later

This section provides the information about setting options in Internet Explorer 9.0 and later before running Avaya Agent Web Client.

Note:

Do not access another website in new tab of the same Internet Explorer instance from which you accessed Avaya Agent Web Client login page.

To set the options in Internet Explorer 9.0 and later:

1. Add Avaya Agent Web Client IP address in the **Compatibility View Settings** of the Internet Explorer.
2. From the system, uninstall Avaya WindowManager Control if it is already installed.
   a. Open the Internet Explorer browser.
   b. From the main menu, select **Tools** > **Internet Options**.
   c. On the **General** tab, click **Settings** in the **Browsing History** area.
   d. Click **View Objects** to view if Avaya WindowManager Control is already installed.
   e. Right-click **Avaya WindowManager Control** if present, and select **Remove**.

      The system uninstalls the Avaya WindowManager Control software.
3. Set the Internet Explorer so that Avaya Agent Web Client works correctly.
   a. From the main menu of Internet Explorer, select **Tools** > **Internet Options**.
   b. Click **Advanced** tab.
   c. In the Accessibility section, select the **Reset text size to medium for new windows and tabs** check box.
   d. In the Browsing section, clear the **Enable automatic crash recovery** and **Enable third-party browser extensions** check boxes.
   e. In the Browsing section, select the following check boxes:
      - Close unused folders in History and Favorites
      - Disable script debugging (Internet Explorer)
      - Enable FTP folder view (outside of Internet Explorer)
      - Enable suggested Sites
      - Load sites and content in the background to optimize performance
      - Notify when downloads complete
      - Show freindly HTTP error messages
      - Underline links - Always
      - Use inline AutoComplete in the Internet Explorer Address Bar and Open Dialog

- Use Passive FTP (for firewall and DSL modem compatibility)
- Use smooth scrolling

f. In the HTTP settings section, select **Use HTTP 1.1** and **Use HTTP 1.1 through proxy connections** check boxes.

g. In the International section, select **Send IDN server names for non-Intranet URLs**, **Send URL path as UTF-8**, and **Show Notification bar for encoded addresses** check boxes.

h. In the Multimedia section, select the following check boxes:

- Enable alternative codecs in HTML5 media elements
- Enable automatic image resizing
- Play animations in webpages
- Play sounds in webpages

i. In the Security section, select the following check boxes:

- Check for signatures on downloaded programs
- Enable native XMLHTTP support
- Send Do Not Track requests to sites you visit in Internet Explorer
- Use SSL 3.0
- Use TLS 1.0
- Warn about certificate address mismatch
- Warn if POST submittal is redirected to a zone that does not permit posts

j. On the **General** tab, click **Tabs**. The system displays **Tabbed Browsing Settings** dialog box.

k. In the Tabbed Browsing area, select the following check boxes:

- Warn me when closing multiple tabs
- Show previews for individual tabs in the taskbar
- Enable Tab Groups

l. In the **When a pop-up is encountered** area, select **Always open pop-ups in a new window** check box.

m. In the **Open links from other programs in** area, select **A new tab in the current window** check box.

n. Click **OK**.

o. In the **Internet Options** dialog box, click **OK**.

4. Restart the Internet Explorer browser.
5. Access Avaya Agent Web Client.

6. Select install if the system displays a prompt for installing the `avayaicagent.cab` file.
7. After the `avayaicagent.cab` file is installed, close Internet Explorer.

Testing Avaya Agent Web Client

Note:
For information about Avaya Agent Web Client log files and troubleshooting issues, see *Interaction Center Administration Guide*.

To test Avaya Agent Web Client:

1. In a Web browser, navigate to the following URL:

   http://*WEB_CONNECTOR_SERVER_NAME*:9080/avaya/agent/login.jsp

   where ***WEB_CONNECTOR_SERVER_NAME*** is the fully qualified domain name of the system that hosts Web Connector.

   Note:
   Ensure that the Web Client Connector server is reachable from the workstation of an agent.
2. Log in to Avaya Agent Web Client with the login ID and password of an agent in the IC system.

Advance Configuration

This section includes the following topics:

- Configuring SSL security for Avaya Agent Web Client (optional) on page 466
- Verifying the deployment of AAWC on page 468
- Verifying the deployment of AAWC on page 468

Configuring SSL security for Avaya Agent Web Client (optional)

To enable the AAWC server for SSL perform the following steps:

1. Stop AAWC. Change the directory to: `<IC_INSTALL_DIR\IC73>\bin`.
   - aawcclient.bat stop
   - ./aawcclient.sh stop
2. Back up the file *`IC_INSTALL_DIR`*`\IC73\tomcat\conf\server.webclient.xml`

3. In a text editor, such as Notepad, open the following server configuration file: *IC_INSTALL_DIR*\IC73\tomcat\conf\server.webclient.xml
4. In the file, comment the default HTTP connector and uncomment the HTTPS connector. HTTPS connector can be located by searching for the XML tag with the following attribute: `sslProtocol="TLS"`
5. (Optional) Add the `SSLEnabled="true"` attribute in the previous XML tag.

   From IC 7.3.3 onwards, `SSLEnabled="true"` attribute is added by default in the `server.icwebservices.xml` file.
6. Specify the SSL protocols by adding the following attribute in the same tag:

   `sslProtocol="TLS"`

   From IC 7.3.5 onwards, set the `sslProtocol` attribute to `sslProtocol="TLSv1.2".`

   Also, set the `sslEnabledProtocols` attribute to the list of supported SSL protocols (protocols not listed in the supported SSL protocols list are disabled):

   `sslEnabledProtocols="TLSv1.2"`

   This setting avoids poodle vulnerability.
7. Substitute the appropriate values for the following attributes of that tag:
   - keystoreFile (keystore file location)
   - keystorePass (keystore file access password)

     For example,

     ```
     <Connector port="9043" acceptCount="1025"
     connectionTimeout="300000" disableUploadTimeout="true"
     maxThreads="300" maxHttpHeaderSize="8192" scheme="https"
     secure="true" SSLEnabled="true" sslProtocol="TLSv1.2"
     sslEnabledProtocols="TLSv1.2" keystoreFile="C:\Avaya\
     keystorefile" keystorePass="changeit" />
     ```

   Note:
   For more information on poodle vulnerability, see Apache website.
   For more information about setting up tomcat for SSL, go to http://tomcat.apache.org and search for SSL.
8. Change Directory *IC_INSTALL_DIR*\IC73\bin and edit `aawcclient.bat`.

   Note:
   Perform a backup before editing.
9. Change the AVAYA_IC_WEBCLIENT_URL value to start with https.
10. To start AAWC, change the directory to: `<IC_INSTALL_DIR\IC73>\bin`.
    - aawcclient.bat start
    - ./aawcclient.sh start.

Note:

For more information about setting up tomcat for SSL, go to http://tomcat.apache.org and search for SSL.

Verifying the deployment of AAWC

To verify the successful deployment of AAWC:

1. Verify that `aawcclient.bat` or `aawcclient.sh`, located in the *`IC_INSTALL_DIR`*`\IC73\bin` folder, is updated with the changes you have provided in the configtool.
2. Check whether JavaAppBridge server status is showing `Up`.
3. Check the *`IC_INSTALL_DIR`*`\IC73\tomcat\webapps\Avaya` directory for the agent folder that contains subfolder and files.
4. Check whether Windows Task Manager is showing the `javaw` process running.
5. Check whether Alarm Monitor has generated an information alarm **The application started successfully**.

Redeploying the application WAR file

You can update or customize Web Client and redeploy the application WAR file without uninstalling all Avaya Agent Web Client components.

Run the following procedure on the Web Client Connector system to redeploy the application WAR file:

1. Stop the Avaya Agent Web Client if it is running. For more information, see Starting and stopping Avaya Agent Web Client on page 463.
2. On the WebConnector system, go to the *`Avaya IC Home`*`\bin` directory.
3. Run the command: **`aawcclient.bat stop`**
4. From Windows Task Manager, ensure that the `javaw.exe` process is not running.
5. Back up the existing `webclient.war` file available in the `Tomcat\Avaya\war` directory.
6. Delete the `avaya#agent` folder from the `Tomcat/webapps` directory.
7. Generate a new war file as described in Creating the application WAR file on page 449.
8. Copy the new generated war file from the Avaya Agent Web Client system to the `Tomcat/Avaya/war` directory of the Web Client Connector system.
9. On the WebConnector system, go to the *`Avaya IC Home`*`\bin` directory.

10. Run the command: **`aawcclient.bat start`**
11. From Windows Task Manager, verify that the JAB server is Up and running.

Chapter 17: Deploying Client SDK components

This section includes the following topics:

1. Before you deploy Client SDK components on page 470
2. Installing the Client SDK components on page 471
3. Configuring a secondary ORB server environment on page 472
4. Client SDK files on page 472
5. Setting up the Java Application Bridge on page 473
6. Configuring Client SDK services on page 476
7. Starting and stopping the Client SDK server on page 477
8. Enabling the SDK server for SSL (optional) on page 478
9. Running a sample client on page 480
10. Optional advanced configuration for the Client SDK server on page 482

Important:
Read the IC Readme and *Avaya IC Installation Planning and Prerequisites* before you deploy the Client SDK.

Before you deploy Client SDK components

Before you deploy Client SDK server or design components:

- Install the required third-party software, as described in *Avaya IC Installation Planning and Prerequisites*.
- Install and configure all IC prerequisites, as described in *Avaya IC Installation Planning and Prerequisites*.
- Install and configure Avaya IC, including all media channels and Avaya FTSE.
- Create and configure agent accounts for agents who are using custom applications developed with the Client SDK, as described in Configuring agent accounts on page 374.

Installing the Client SDK components

Install the Client SDK server and design components, as described in Installing IC server components on page 35.

Tip:
You can install client SDK server component on IC core server system. To install client SDK server component on IC core server system you require additional 2GB ram added in the server configuration as compared to the specified memory value of IC core host system.

The following table lists the Client SDK components installed with each operating system.

Operating system	Deployment
Windows	Installs the following components: • Client SDK server components • Java and .NET design components
Solaris	Installs the following components: • Client SDK server components • Java design components To get the .NET design components, you must install the Client SDK on a Windows system.
AIX	Installs the following components: • Client SDK server components • Java design components To get the .NET design components, you must install the Client SDK on a Windows system. **Note:** IBM AIX and IBM DB2 are only supported on Interaction Center Release 7.3, 7.3.1, and 7.3.2. For more information see the Supported Server Operating Systems section in the Avaya IC Installation Planning and Prerequisites Guide. All the information related to IBM AIX and IBM DB2 is only applicable to Interaction Center Release 7.3, 7.3.1, and 7.3.2.

Configuring a secondary ORB server environment

The Client SDK server requires a secondary ORB server. Configure a secondary server environment, as described in Configuring a secondary ORB server environment on page 47.

Client SDK files

The following table describes the contents of the SDK directories created when you install the Client SDK components.

Directory	Contents
sdk/server	Client SDK server files, including the WAR file for Tomcat
sdk/design	All design files for the Client SDK in the following directories: • dotnet • java The following diagrams in PDF format: • Object model • State models for all stateful Client SDK objects
sdk/design/dotnet/lib	C# client libraries for the Client SDK client
sdk/design/dotnet/sample	Source code and binaries for the .NET sample client
sdk/design/dotnet/doc	Client API reference documentation for the `.NET` API
sdk/design/java/lib	Java client libraries for the Client SDK client
sdk/design/java/sample	Source code and binaries for the Java sample client
sdk/design/java/doc	Client API reference documentation for the Java API.

Setting up the Java Application Bridge

The Client SDK server uses the Java Application Bridge to communicate with the IC servers and databases.

This section includes the following topics:

1. Creating an agent account for the Java Application Bridge on page 473
2. Creating a Java Application Bridge on page 474

Creating an agent account for the Java Application Bridge

The Java Application Bridge requires a non-human agent account for IC. You use this agent account when you configure Tomcat for the Client SDK server. This account is the DCO Bridge account.

The IC seed data includes one non-human agent account for the DCO Bridge. You can use this account for the first Java Application Bridge in the IC system.

You must create a unique non-human agent account for each additional Java Application Bridge in the IC system. You must name each account dcobridge*N*. The agent name can also include the name of the system that hosts the Java Application Bridge.

Tip:
The following instructions describe how to create additional non-human agent accounts for the Java Application Bridge. If you use the account in the IC seed data, double-click that agent account and complete Step 5 below.

To create an agent account for the Java Application Bridge:

1. In IC Manager, click the **Agent** tab.
2. In the left pane, expand the **DefaultTenant** node.

   If you want to create the agent account in a different tenant, expand that node in the left pane instead of **DefaultTenant**.
3. Select **Agent** > **New**.
4. Click the **General** tab and enter the information for the fields mentioned in the following fields:

Field	Recommended entry
First Name	dcobridge*N* (for example, dcobridge2)
Last Name	dcobridge*N* (for example, dcobridge2)

Field	Recommended entry
Preferred Name	dcobridge*N* (for example, dcobridge2)
Employee ID	dcobridge*N* (for example, dcobridge2)
Login ID	dcobridge*N* (for example, dcobridge2)
Domain	The same user domain as the Java Application Bridge that will use this agent account. For example, User1.
Task Load	0
Task Ceiling	0
Site	DefaultSite

5. Click the **Security** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry
Password	Enter a password for this account. **Tip:** Change the password for the pre-defined Java Application Bridge account.
Confirm	Re-enter the password for this account.
Force password change on login	Clear this field. Do not select this field for non-human IC users
Disable login	Do not select this field.
Role	Select the **Agent** role. **Note:** Do not select any of the other roles.

6. Click **OK**.

Creating a Java Application Bridge

You must create a Java Application Bridge on the Client SDK server system. The Java Application Bridge is not a true IC server. The Java Application Bridge impersonates each agent who logs in to the Client SDK. When the Java Application Bridge makes a request for an agent, the Java Application Bridge mirrors the domain structure of the agent.

To create a Java application bridge:

1. In IC Manager, click the **Server** tab.

2. Select **Server** > **New**.
3. From the list of servers, select **JavaAppBridge**.
4. Click **Ok**.
5. Click the **General** tab and enter the information for fields mentioned in the following table.

Field	Recommended entry	Notes
Name	Enter a name for the Java Application Bridge.	Include the name of the system that hosts the Tomcat application server to identify the location of the JavaAppBridge.
Domain	Select an IC User domain for the Java Application Bridge from the drop-down list.	For example, select `User1` from the drop-down list. Assign the Java Application Bridge to the same User domain as most Client SDK application users. You do not need a Java Application Bridge in each User domain. Ensure that the domain with the Java Application Bridge fails over to the following domains: • Itself • Default domain • All domains with an ADU server
Host	Enter the IP address of the system that hosts the Client SDK server.	
Port	Enter a port assignment for the Java Application Bridge.	You can use any available port in the 9000 range for the Java Application Bridge. Use port 9002.
Directory	Enter the path to the `etc` directory for the Client SDK server.	For example, enter: *IC_INSTALL_DIR*\IC73\etc where *IC_INSTALL_DIR* is the path to this directory on the Client SDK server system. For example, if you used the default, the path is: C:\Avaya\IC73\etc
Executable	Enter `jabsrv`.	Leave the default entry. **Tip:** This entry exists because Executable is a required field in IC Manager. No separate executable exists for the Java Application Bridge.

6. Record the **Name** value for the Java Application Bridge. You need this name in Configuring Client SDK services on page 476.
7. Click the **JavaAppBridge** tab and enter the information for the fields mentioned in the following table.

Field	Recommended entry	Notes
IC User	Enter the name of the agent account for this Java Application Bridge server.	Use the account that you created in Creating an agent account for the Java Application Bridge on page 473. For example, enter dcobridge1.
IC Password	Enter the password associated with the agent account.	

8. Click **OK**.

Important:
Do not start the Java Application Bridge in IC Manager. When you start the Client SDK server in Tomcat, that server starts the Java Application Bridge.

Configuring Client SDK services

Configure Client SDK services on all systems that host Client SDK server or design components.

To configure Client SDK services:

1. Start the Configuration Tool:

Operating system	Procedure
Windows	Select **Start** > **Programs** > **Avaya Interaction Center 7.3** > **Configuration Tool**.
Solaris	1. Navigate to *IC_INSTALL_DIR*/IC73/bin 2. Run **./configure**
AIX	1. Navigate to *IC_INSTALL_DIR*/IC73/bin 2. Run **./configure**

2. Log in with your IC Manager login ID and password.

3. Click the **SDK Server** tab.
4. In the **SDK Server System** field, type the fully-qualified domain name of the system that hosts the Client SDK server.
5. In the **JavaAppBridge Name** field, type the name of the Java Application Bridge that this Client SDK server will use.
6. Click **Apply Settings**.
7. Click **Exit**.

Starting and stopping the Client SDK server

This section includes the following topics:

- Starting and stopping the Client SDK server on Windows on page 477
- Starting and stopping the Client SDK server on Solaris on page 478
- Starting and stopping the Client SDK server on AIX on page 478

Starting and stopping the Client SDK server on Windows

To start, stop and configure the Client SDK server on Windows:

1. In the Services control panel, right-click on the Avaya IC 7.3 SDK Service.
2. From the right-click menu, select one of the options in the following table:

Task	Options
Start Client SDK server	Select **Start**.
Stop Client SDK server	Select **Stop**.
Set startup options	1. Select **Properties**. 2. Select **Automatic** from the **Startup Type** drop-down list. 3. Click **OK**.

Starting and stopping the Client SDK server on Solaris

Execute all Client SDK server commands from the *IC_INSTALL_DIR*/IC73/bin directory. For the Client SDK server to be able to log in, the IC servers must be started first.

Starting the Client SDK server: To start the Client SDK server, execute the following command:

```
nohup ./ictomcat.sh start SDK
```

Stopping the Client SDK server: To stop the Client SDK server, execute the following command where -force is an optional parameter that terminates the server processes:

```
nohup ./ictomcat.sh stop SDK -force
```

Starting and stopping the Client SDK server on AIX

Execute all Client SDK server commands from the *IC_INSTALL_DIR*/IC73/bin directory. For the Client SDK server to be able to log in, the IC servers must be started first.

Starting the Client SDK server: To start the Client SDK server, execute the following command:

```
nohup ./ictomcat.sh start SDK
```

Stopping the Client SDK server: To stop the Client SDK server, execute the following command where -force is an optional parameter that terminates the server processes:

```
nohup ./ictomcat.sh stop SDK -force
```

Enabling the SDK server for SSL (optional)

Perform the following changes on the server to enable the SDK server for SSL:

1. Stop SDK Services.
   - In the Services control panel, right-click the "Avaya IC 7.3 SDK" and select **stop**.
   - Change the directory *IC_INSTALL_DIR*\IC73\bin and execute the nohup ./ictomcat.sh stop SDK -force command.
2. Back up the *IC_INSTALL_DIR*\IC73\tomcat\conf\server.icsdk.xml file.
3. In a text editor, such as Notepad, open the *IC_INSTALL_DIR*\IC73\tomcat\conf\server.icsdk.xml server configuration file.
4. Search for the XML tag with the sslProtocol="TLS" attribute and remove the HTML comment mark from that XML tag.

5. (Optional) Add the `SSLEnabled="true"` attribute in the same XML tag.

   From IC 7.3.3 onwards, `SSLEnabled="true"` attribute is added by default in the `server.icwebservices.xml` file.

6. Specify the SSL protocols by adding the following attribute in the same tag:

   `sslProtocol="TLS"`

   From IC 7.3.5 onwards, set the `sslProtocol` attribute to `sslProtocol="TLSv1.2".`

   This setting avoids poodle vulnerability.

7. Substitute the appropriate values for the following attributes of that ttag:
   - keystoreFile (keystore file location)
   - keystorePass (keystore file access password)

     For example,

     ```
     <Connector port="9743" acceptCount="1025"
     connectionTimeout="300000" disableUploadTimeout="true"
     maxThreads="300" maxHttpHeaderSize="8192" scheme="https"
     secure="true" SSLEnabled="true" sslProtocol="TLSv1.2"
     keystoreFile="C:\Avaya\keystorefile" keystorePass="changeit" />
     ```

Note:
For more information on poodle vulnerability, see Apache website.
For more information about setting up tomcat for SSL, go to http://tomcat.apache.org and search for SSL.

8. Start SDK Services.
   - In the Services control panel, right-click **Avaya IC 7.3 SDK** and select **Start**.
   - Change the directory *IC_INSTALL_DIR*`\IC73\bin` and execute the `nohup ./ictomcat.sh Start SDK` command.

Note:
For more information about setting up tomcat for SSL, goto the Apache website and search for SSL.

Configuring SDK Server with SSL on Java and Dotnet platform

You must follow the following procedure.

For enabling the SDK server for SSL (optional).

1. You need to Add the SSLEnabled="true" attribute in the same XML tag. From IC 7.3.3 onwards, SSLEnabled="true" attribute is added by default in the server.icsdk.xml file. You need to change server.icsdk.xml file.

   Note: For SDK Clients for Windows/Solaris (AIX is not supported anymore)

   Note**:** For Enabling the .NET sample client for SSL on Windows**.**

Importing the certificate for .NET Sample SDK Client in the Windows MMC console

This procedure is not required in case the CA root authority is a trusted certifying authority such as VeriSign or Thawte that has signed the server certificate. This procedure is required only for the self-signed server certificate.
Before you import the certificate, copy the exported server certificate to the system where it is imported. You must import the certificate to machines from where you run the .NET sample client.CN in the certificate should match the hostname used in the URL to access the server.

To import CA certificate in the Windows MMC console:

1. Click on the **Start menu > Run**.
2. In the Open field, type **mmc** and click **OK**.
3. Click **File** and then click **Add/Remove Snap-in**...
4. Double-click on certificates.
5. Click **Computer Account** and then click **Next**.
6. Leave Local Computer selected and click **Finish**.
7. Click **OK**.
8. Click the plus sign next to Certificates in the left pane.
9. Click the plus sign next to Trusted Root Certification Authorities and click the **Certificates** folder. Right Click, All Tasks and then **Import**…
10. In the **Certificate Import Wizard**, click **Next**.
11. Click **Browse** and select the certificate file which has the CA root certificate that you copied.
Click **Open** and then **Next**.
12. Click the **Place all the certificates in the following store**: **Trusted Root Certification Authorities** option**.**
13. Click **Next**.
14. Click **Finish** to complete the wizard.
The certificate is now listed as one of the trusted root certificate.
15. Close the **MMC** console.

Importing the certificate for Java Sample SDK Client in the JAVA Keystore

Before you import the certificate, copy the exported server certificate to the system where it will be imported. You must import the certificate to machines from where you run the Java sample client.
The CA root authority certificate needs to be imported in the Java keystore as Java sample client uses JRE's database of trusted certificates. This will allow Java sample client to trust the certificate coming from SDK server during SSL handshake.

To import the CA certificate in the JAVA Keystore on machine where Java sample client is configured for SSL:

1.Copy the server certificate to Java sample client machine on `%AVAYA_IC73_HOME%\sdk\design\java\sample\bin folder`.

2. Open the command prompt and run following commands to import above certificate:
    - `cd %AVAYA_IC73_HOME%\sdk\design\java\sample\bin.`
    - `%AVAYA_IC73_HOME%\Java\bin\keytool.exe -import -file`

```
<CERTIFICATE> -alias <ALIAS> -keystore <KEYSTORE> -
storepass <PSWD>
```

3. e.g.: keytool.exe -import -file C:\icsdk.crt -alias icsdkkey -keystore C:\truststore -storepass 123
4. When prompted to trust the certificate, click **Yes**.
5. Verify that the keystore has successfully imported the CA certificate by checking the output of following command:

   ```
   %AVAYA_IC73_HOME%\Java\bin\keytool.exe -list -v -alias <ALIAS> -
   keystore <KEYSTORE> -storepass <PSWD>
   ```

Note: All the keystore entries (key and trusted certificate entries) are stored and accessed using unique, case-insensitive aliases through the keystore. If certificate alias name is not provided, then the default alias name mykey is used by the keytool.

Running the Java sample client with SSL enabled on Windows

You need to change and run `RunClient.bat`

```
REM %DIR%\java -cp "%CLASSPATH%" com.avaya.ic.sdk.sample.SampleClient
%DIR%\java -cp "%CLASSPATH%" -Djavax.net.ssl.trustStore=<KEYSTORE> -
Djavax.net.ssl.trustStorePassword=<PSWD>
com.avaya.ic.sdk.sample.SampleClient
```

For Example:

```
%DIR%\java -cp "%CLASSPATH%" -Djavax.net.ssl.trustStore=C:\truststore -
Djavax.net.ssl.trustStorePassword=123
com.avaya.ic.sdk.sample.SampleClient
```

Importing the certificate for Java Sample SDK Client in the JAVA Keystore

Before you import the certificate, copy the exported server certificate to the system where it will be imported. You must import the certificate to machines from where you run the Java sample client.

The CA root authority certificate needs to be imported in the Java keystore as Java sample client uses JRE's database of trusted certificates. This allows Java sample client to trust the certificate coming from SDK server during SSL handshake.

To import the CA certificate in the JAVA Keystore on machine where Java sample client is configured for SSL:

1. Copy the server certificate to Java sample client machine on `%AVAYA_IC73_HOME%/sdk/design/java/sample/bin folder`.
2. Open the command prompt and run following commands to import above certificate:

a. `cd %AVAYA_IC73_HOME%/sdk/design/java/sample/bin`

b. `%AVAYA_IC73_HOME%/Java/bin/keytool -import -file <CERTIFICATE> -alias <ALIAS> -keystore <KEYSTORE> -storepass <PSWD>`

For example:

i. `/export/home/Avaya/IC73/Java/bin/keytool -import -file /export/home/Avaya/IC73/sdk/design/java/sample/bin/icsdk.crt -alias icsdkkey -keystore /export/home/Avaya/IC73/sdk/design/java/sample/bin/truststore -storepass 123`

3. When prompted to trust the certificate, click **Yes**.
4. Verify that the keystore has successfully imported the CA certificate by checking the output of following command:

i. `%AVAYA_IC73_HOME%/Java/bin/keytool -list -v -alias <ALIAS> -keystore <KEYSTORE> -storepass <PSWD`

Running the Java sample client with SSL enabled on Solaris

Change and run `runclient.sh` as follows:

```
#$DOLLAR$DIR/java -cp $DOLLAR$CLASSPATH
"com.avaya.ic.sdk.sample.SampleClient"
$DOLLAR$DIR/java -cp $DOLLAR$CLASSPATH -
Djavax.net.ssl.trustStore=<KEYSTORE> -
Djavax.net.ssl.trustStorePassword=<PSWD>
"com.avaya.ic.sdk.sample.SampleClient"
```

For example:

```
$DOLLAR$DIR/java -cp $DOLLAR$CLASSPATH -
Djavax.net.ssl.trustStore=/export/home/Avaya/IC73/sdk/design/java/sample/
bin/truststore -Djavax.net.ssl.trustStorePassword=123
"com.avaya.ic.sdk.sample.SampleClient"
```

Running a sample client

Perform these procedures on the development system where you installed the Client SDK components. For more information about the Client SDK sample clients, see *Avaya IC Client SDK Programmer Guide*.

This section includes the following topics:

- Running the .NET sample client on Windows on page 480
- Running the Java sample client on Windows on page 480
- Running the Java sample client on Solaris on page 481
- Running the Java sample client on AIX on page 481

Running the .NET sample client on Windows

To run the `.NET` sample client on a Windows system:

1. select **Start** > **Programs** > **Avaya Interaction Center** 7.3 > **Run .Net Sample Client**.
2. In the dialog box, enter:
   - URL for the Client SDK server

     The URL must use the format: `http://<SDK_Server_System_Name>:<Port>/<Application_context>`. For example, with the default configuration, the URL could be `http://testbox.xyzcorp.com:9700/icsdk`
   - IC agent account
   - Password for the IC agent account
3. Click **Ok**.

Running the Java sample client on Windows

To run the Java sample client on a Windows system:

1. Select **Start** > **Programs** > **Avaya Interaction Center** 7.3 > **Run Java Sample Client**.
2. In the dialog box, enter:
   - URL for the Client SDK server

     The URL must use the format: `http://<SDK_Server_System_Name>:<Port>/<Application_context>`. For example, with the default configuration, the URL could be `http://testbox.xyzcorp.com:9700/icsdk`
   - IC agent account
   - Password for the IC agent account

3. Click **Ok**.

Running the Java sample client on Solaris

To run the Java sample client on the Solaris system:

1. Navigate to the following folder:

   IC_INSTALL_DIR\IC73\sdk\design\java\sample\bin
2. Execute the following command: ./**runclient.sh**
3. In the dialog box, enter:
   - URL for the Client SDK server

     The URL must use the format: `http://<SDK_Server_System_Name>:<Port>/<Application_context>`. For example, with the default configuration, the URL could be `http://testbox.xyzcorp.com:9700/icsdk`
   - IC agent account
   - Password for the IC agent account
4. Click **Ok**.

Running the Java sample client on AIX

To run the Java sample client on the AIX system:

1. Navigate to the following folder:

   IC_INSTALL_DIR\IC73\sdk\design\java\sample\bin
2. Execute the following command: ./**runclient.sh**
3. In the dialog box, enter:
   - URL for the Client SDK server

     The URL must use the format: `http://<SDK_Server_System_Name>:<Port>/<Application_context>`. For example, with the default configuration, the URL could be `http://testbox.xyzcorp.com:9700/icsdk`
   - IC agent account
   - Password for the IC agent account
4. Click **Ok**.

Optional advanced configuration for the Client SDK server

This section includes the following topics:

- Configuring the log4j files for the Client SDK server (optional) on page 482
- Changing default port range (optional) on page 483

Configuring the log4j files for the Client SDK server (optional)

To configure the log4j files for the Client SDK server:

1. In a text editor, open the following file:

   IC_INSTALL_DIR\IC73\tomcat\bin\icsdk.bat

2. Navigate to the section between MODIFICATION SECTION BEGIN and MODIFICATION SECTION END.
3. Update the following parameters in this section:

Parameter	Notes
LOG4J_CONFIGURATION	Enter the full path and file name for the Log4j XML file.
LOG4J_DEBUG	Set the Log level as follows: • **true** to enable logging • **false** to disable logging
JAVA_SECURITY_AUTH_LOGIN_CONFIG	Enter the full path to the directory that contains the cup.security file. For example: **AVAYA_IC73_HOME\SDK\cup.security**

4. Save the `icsdk.bat` file.

Changing default port range (optional)

By default, the Client SDK server accepts connections from a client in a port range between 8000 and 9000. If a client is outside the firewall, you must open up ports in this range.

You can change the port range in the web.xml file.

To change the default port range:

1. Open `web.xml` in a text editor.

   You can find the `web.xml` file in the `IC_INSTALL_DIR\IC73\sdk\server\icsdk\WEB-INF` folder.

2. Search for the `messaging.listener.port.range` entry.

   This entry does not exist out-of-the-box.

3. If the entry does not exist, add the `messaging.listener.port.range` entry to the web.xml file.

4. Set the value of `messaging.listener.port.range` entry to the required port range, as follows:

   <a>-<b>

   where the value of a is greater than the value of b, and where a and b are unsigned integers which represent a valid port range. For example, a valid value is 9050-8050.

5. Save the file.

6. Restart the Tomcat server, as described in Starting and stopping the Client SDK server on Windows on page 477.

Chapter 18: Deploying Web Services

This section includes the following topics:

- Before you deploy Web Services components on page 484
- Installing the Web Services components on page 485
- Configuring a secondary ORB server environment on page 485
- Web Services files on page 485
- Setting up the Web Services Bridge on page 485
- Configuring Web Services on page 490
- Starting and stopping the Web Services server on page 491

Important:
Read the IC Readme and *Avaya IC Installation Planning and Prerequisites* before you deploy Web Services.

Before you deploy Web Services components

Before you deploy Web Services components:

- Install the required third-party software, as described in *Avaya IC Installation Planning and Prerequisites*.
- Install and configure all IC prerequisites, as described in *Avaya IC Installation Planning and Prerequisites*.
- Install and configure Avaya IC, including all media channels and Avaya FTSE.
- Create and configure agent accounts for agents who use Web Services, as described in Configuring agent accounts on page 374.

Installing the Web Services components

Install the Web Services components, as described in Installing IC server components on page 35.

Configuring a secondary ORB server environment

The Web Services server requires a secondary ORB server. Configure a secondary server environment, as described in Configuring a secondary ORB server environment on page 47.

Web Services files

The following table describes the contents of the SDK directories created when you install the Web Services components.

Directory	Contents
sdk/WebServices	Web Services server files, including the WAR file for Tomcat
sdk/webservices/sample	Sample Web Services client files

Setting up the Web Services Bridge

The Web Services server uses the Web Services Bridge to communicate with the IC servers and databases.

This section includes the following topics:

1. Creating an agent account for the Web Services Bridge on page 486
2. Creating a Web Services Bridge on page 487

Creating an agent account for the Web Services Bridge

The Web Services Bridge requires a non-human agent account for IC. You use this agent account when you configure Tomcat for the Web Services server. This account is a DCO Bridge account.

You must create a unique non-human agent account for each Web Services Bridge in the IC system. Name each account dcobridge*N*. The agent name can also include the name of the system that hosts the Web Services Bridge.

To create an agent account for the Web Services Bridge:

1. In IC Manager, click the **Agent** tab.
2. In the left pane, expand the **DefaultTenant** node.

   If you want to create this agent account in a different tenant, expand that node in the left pane instead of **DefaultTenant**.
3. Select **Agent** > **New**.
4. Click the **General** tab and enter the information for the fields mentioned in the following fields:

Field	Recommended entry
First Name	dcobridge*N* (for example, dcobridge2)
Last Name	dcobridge*N* (for example, dcobridge2)
Preferred Name	dcobridge*N* (for example, dcobridge2)
Employee ID	dcobridge*N* (for example, dcobridge2)
Login ID	dcobridge*N* (for example, dcobridge2)
Domain	The same user domain as the Web Services Bridge that use this agent account. For example, User1.
Task Load	0
Task Ceiling	0
Site	DefaultSite

5. Click the **Security** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry
Password	Enter a password for this account.
Confirm	Re-enter the password for this account.
Force password change on login	Clear this field. Do not select this field for non-human IC users
Disable login	Do not select this field.
Role	Select the **Agent** role. **Note:** Do not select any of the other roles.

6. Click **OK**.

Creating a Web Services Bridge

You must create a Web Services Bridge on the Web Services server system. The Web Services Bridge is not a true IC server.

To create a Web Services Bridge:

1. In IC Manager, click the **Server** tab.
2. Select **Server** > **New**.
3. From the list of servers, select **WebServices**.
4. Click **Ok**.
5. Select the **General** tab and complete the fields shown in the following table.

Field	Recommended entry	Notes
Name	Enter a name for the Web Services Bridge.	Include the name of the system that hosts the Tomcat application server to identify the location of the Web Services Bridge.

Field	Recommended entry	Notes
Domain	Select an IC User domain for the Web Services Bridge from the drop-down list.	For example, select `User1` from the drop-down list. Ensure that the domain with the Web Services Bridge fails over to the following domains: • Itself • Default domain • All domains with an ADU server
Host	Enter the IP address of the system that hosts the Web Services server.	
Port	Enter a port assignment for the Web Services Bridge.	You can use any available port in the 9000 range for the Web Services Bridge. Use port 9003.
Directory	Enter the path to the `etc` directory for the Web Services server.	For example, enter: *IC_INSTALL_DIR*\IC73\etc where *IC_INSTALL_DIR* is the path to this directory on the Web Services server system. For example, if you used the default, the path is: C:\Avaya\IC73\etc
Executable	Enter `wssrv`.	Leave the default entry. **Tip:** This entry exists because **Executable** is a required field in IC Manager. No separate executable exists for the Web Services Bridge.

6. Record the **Name** value for the Web Services Bridge. You need this name in Configuring Web Services on page 490.
7. Select the **WebServices** tab and complete the fields as described in the following table:

Field	Recommended entry	Notes
IC User	Enter the name of the agent account for this Web Services Bridge.	Use the account that you created in Creating an agent account for the Web Services Bridge on page 486. For example, enter dcobridge1.
IC Password	Enter the password associated with the agent account.	
Enable SSL for DS Authentication	If 'Enable SSL for DS Authentication' configuration parameter is selected, DS.Authenticate request is sent over SSL by WebServices to DS in SSL encrypted format. It supports authentication for both LDAP and non-LDAP users. If 'Enable SSL for DS Authentication' configuration parameter is cleared, DS.Authenticate request is sent over VESP by WebServices to DS. The password is in MD5 encrypted format and rest of the request parameters are in plain text format in this case. It supports authentication for ONLY non-LDAP users and authentication for LDAP users might fail.	• The response time for DS.Authenticate over SSL is slower compared to the response time of DS.Authenticate over VESP because of the SSL overhead of handshake, encryption/decryption and so on. • If 'Enable SSL for DS Authentication' configuration parameter is cleared, DS.Authenticate request for the LDAP-enabled users might fail. To authenticate the LDAP-enabled users, DS.Authenticate must be sent over SSL by checking 'Enable SSL for DS Authentication' configuration parameter.
Skip ADU Events for WebServices User		Selecting this option prevents the Webservice server from receiving the ADU events. By default, the option is cleared and the server receives ADU events.

8. Click **Ok**.

Important:
Do not start the Web Services Bridge in IC Manager. When you start the Web Services server in Tomcat, that server starts the Web Services Bridge.

Configuring Web Services

Configure Web Services on all systems that host Web Services components.

To configure Web Services:

1. In a text editor, open the following file:
   - *IC_INSTALL_DIR*\IC73\tomcat/bin/icwebservices.bat
   - *IC_INSTALL_DIR*/IC73/tomcat/bin/icwebservices.sh
   - *IC_INSTALL_DIR*/IC73/tomcat/bin/icwebservices.sh
2. Navigate to the section between MODIFICATION SECTION BEGIN and MODIFICATION SECTION END.
3. Update the following parameters in this section to match your development environment:

Parameter	Notes

AVAYA_IC_WEBCLIENT_URL	Enter the correct protocol, host name, and port for the system that hosts IC Web Services:
	`http://<ws_System>:[<ws_port>]`
	For example, if you install Web Services on icwsbox.customuser.com, enter:
	`http://icwsbox.customuser.com:9800/`

AVAYA_IC_VESP_ JAVAAPPBRIDGE_NAME	Enter the name of the Web Services Bridge hosted on the system. **Note:** This value is case sensitive.

4. Save the file.
5. Execute the following command on the command prompt to create a Windows service:

   ```
   IC_INSTALL_DIR\IC73\tomcat\bin\icwebservices.bat install
   <ServiceId> <Service Name or Description> server.icsdk.xml
   ```

6. Execute the following command on the command prompt to remove the Windows service:

   ```
   IC_INSTALL_DIR\IC73\tomcat\bin\icwebservices.bat remove
   <ServiceId> <Service Name or Description> server.icsdk.xml
   ```

Starting and stopping the Web Services server

This section includes the following topics:

- Starting and stopping the Web Services server on Windows on page 491
- Starting and stopping the Web Services server on Solaris on page 491
- Starting and stopping the Web Services server on AIX on page 492
- Enabling the Web Services server for SSL on page 492
- Removing IC Web Services on page 493

Starting and stopping the Web Services server on Windows

To start, stop and configure the Web Services server on Windows:

1. In the Services control panel, right-click the IC 7.3 Web Services.
2. From the right-click menu, select one of the options in the following table:

Task	Options
Start Web Services	Select **Start**.
Stop Web Services	Select **Stop**.
Set startup options	1. Select **Properties**. 2. Select **Automatic** from the **Startup Type** drop-down list. 3. Click **Ok**.

Starting and stopping the Web Services server on Solaris

Execute all Web Services server commands from the *IC_INSTALL_DIR*/IC73/bin directory. For the Web Services server to be able to log in, the IC servers must start first.

Starting the Web Services server: To start the Web Services server, execute the following command:

```
nohup ./ictomcat.sh start webservices
```

Stopping the Web Services server: To stop the Web Services server, execute the following command where `-force` is an optional parameter that terminates the server processes:

```
nohup ./ictomcat.sh stop webservices -force
```

Starting and stopping the Web Services server on AIX

Execute all Web Services server commands from the *IC_INSTALL_DIR*/IC73/bin directory. For the Web Services server to be able to log in, the IC servers must start first.

Starting the Web Services server: To start the Web Services server, execute the following command:

```
nohup ./ictomcat.sh start webservices
```

Stopping the Web Services server: To stop the Web Services server, execute the following command where `-force` is an optional parameter that terminates the server processes:

```
nohup ./ictomcat.sh stop webservices -force
```

Enabling the Web Services server for SSL

To enable the Web Services server for SSL, perform the following steps:

1. Stop Web Services:
   - In the Services control panel, right-click the IC 7.3 Web Services and stop the webservice.
   - Change the directory to *IC_INSTALL_DIR*\IC73\bin and execute the following command:

     ```
     nohup ./ictomcat.sh stop webservices -force command
     ```
2. Go to the *IC_INSTALL_DIR*\IC73\tomcat\conf\ directory.
3. From the directory, back up the `server.icsdk.xml` file.
4. In a text editor, such as Notepad, open the `server.icsdk.xml` server configuration file.
5. Search for the XML tag with the `sslProtocol="TLS"` attribute and remove the commenting tag from that XML tag.
6. (Optional) Add the `SSLEnabled="true"` attribute in the previous XML tag.

   From IC 7.3.3 onwards, `SSLEnabled="true"` attribute is added by default in the `server.icsdk.xml` file.

7. Specify the SSL protocols by adding the following attribute in the same tag:

   `sslProtocol="TLS"`

   From IC 7.3.5 onwards, set the `sslProtocol` attribute to `sslProtocol="TLSv1.2".`

   This setting avoids poodle vulnerability.

8. Add the appropriate values for the following attributes of that tag:
   - keystoreFile (keystore file location)
   - keystorePass (keystore file access password)

     For example,

     ```
     <Connector port="9843" acceptCount="1025"
     connectionTimeout="300000" disableUploadTimeout="true"
     maxThreads="300" maxHttpHeaderSize="8192" scheme="https"
     secure="true" SSLEnabled="true" sslProtocol="TLSv1.2"
     keystoreFile="C:\Avaya\keystorefile" keystorePass="changeit" />
     ```

Note:

For more information on poodle vulnerability, see Apache website.
For more information about setting up tomcat for SSL, go to http://tomcat.apache.org and search for SSL.

9. Start Web Services.
   - In the Services control panel, right-click the IC 7.3 Web Services and start the webservice.
   - **`nohup ./ictomcat.sh start webservices.`**
   - **`nohup ./ictomcat.sh start webservices.`**

Note:

For more information about setting up tomcat for SSL, go to the Apache website and search for SSL.

Removing IC Web Services

Perform the following steps to remove the IC Web Services:

1. Stop the already running IC Web Services.
2. Execute the following command on the command prompt to remove Windows service:

   ***IC_INSTALL_DIR*\IC73\tomcat\bin\icwebservices.bat remove <ServiceId>**

Note:

You can find the ServiceId of the installed service through Windows Services Console (services.msc).

3. Delete the *IC_INSTALL_DIR*\IC73\sdk\webservices\webservices folder.

Chapter 19: Uninstalling IC

Uninstalling IC

If you must uninstall IC from a system, perform the following steps to ensure that all services, files, and related components are removed.

1. Uninstalling IC components on Windows on page 496
2. Uninstalling IC servers on Solaris on page 497
3. Uninstalling IC servers on AIX on page 498
4. Uninstalling Web server components on page 498
5. Uninstalling related third-party components on page 499
6. Uninstalling Avaya Agent on page 499
7. Uninstalling Avaya Agent Web Client on page 500

Uninstalling IC components on Windows

Note:

The IC uninstaller occasionally does not remove all entries to the Windows registry. After you uninstall an IC component from a Windows system, you may need to manually remove remaining entries from the Windows Registry.

To uninstall IC components on Windows:

1. In IC Manager, select **Server** > **Shutdown** to stop all IC servers on the system.
2. Close all IC applications on the target system.
3. Stop all IC 7.3 services and the World Wide Web Publishing for IIS service.

   For more information about these services, see Starting and stopping services on Windows on page 114.
4. In the Windows Control Panel:
   a. Open **Add/ Remove Programs**.
   b. Select **Avaya IC 7.3 (*component_name*)**.

      where ***component_name*** is the name of the IC component installed on the system, such as Core Servers, Connector, or Administration.

c. Select **Change/Remove** to start the IC Uninstaller.

Follow the prompts in the IC Uninstaller to uninstall IC services, delete registry settings, and remove files that are not in use.

5. In the Windows Control Panel, delete the IC environment variable:
   a. Double-click **System**.
   b. On the **Advanced** tab, select **Environment Variables**.
   c. Select the IC environment variable in the System Variables box.
   d. Click **Delete**.
   e. Click **Ok**.
6. Delete the remaining folders and files in the *IC_INSTALL_DIR*\IC73\ directory.
7. Delete all shortcuts that you added to the desktop.
8. Open the Windows Registry and confirm that all IC entries have been removed.
9. Continue with Uninstalling Web server components on page 498 without restarting the target system.

Uninstalling IC servers on Solaris

CAUTION:
Do not use the **rm -rf** command to uninstall IC components from Solaris.

To uninstall IC servers on Solaris:

1. Close all IC applications on the target system.
2. In a command window on the target system, stop the IC servers as described in Stopping all servers with the IC Admin utility on page 113.
3. In a command window on the target system, stop the IC services as described in Starting and stopping services on Solaris on page 115.
4. Navigate to *IC_INSTALL_DIR*/IC73/
5. Locate the uninstaller for the component that you want to uninstall.
6. Execute the uninstaller.

   The uninstaller removes all IC related files from the target system, including files that were configured after installation, such as the vesp.imp file.
7. Remove all IC commands that you added to the UNIX startup script.
8. Delete the IC root directory.
9. Continue with Uninstalling Web server components on page 498 without restarting the target system.

Uninstalling IC servers on AIX

CAUTION:
Do not use the **`rm -rf`** command to uninstall IC components from AIX.

To uninstall IC servers on AIX:

1. Close all IC applications on the target system.
2. In a command window on the target system, stop the IC servers as described in Stopping all servers with the IC Admin utility on page 113.
3. In a command window on the target system, stop the IC services as described in Starting and stopping services on AIX on page 118.
4. Navigate to *IC_INSTALL_DIR*/IC73/
5. Locate the uninstaller for the component that you want to uninstall.

   The uninstaller removes all IC related files from the target system, including files that were configured after installation, such as the vesp.imp file.
6. Remove all IC commands that you added to the UNIX startup script.
7. Delete the IC root directory.
8. Continue with Uninstalling Web server components on page 498 without restarting the target system.

Uninstalling Web server components

Perform these steps if the target system includes a Web server. If the target system does not include Web server components, continue with Uninstalling related third-party components on page 499.

To uninstall Web server components:

1. For Tomcat, perform the following steps:
   a. Delete all Tomcat servers that you created to host Web applications, such as the Website and WebLM.
   b. Uninstall Tomcat, if required.
2. For the Web server, perform the following steps:
   a. Remove the virtual directories from your Web site.
   b. For IIS, remove the `dwsensor` and `Jakarta` Connector filters from the **ISAPI Filters** tab.

Uninstalling related third-party components

Perform these steps to complete your uninstallation.

To uninstall related third-party components:

1. Uninstall all related third-party components that you installed on the target system.

   For information on uninstallation procedures, see the manufacturer's documentation.

2. If the target system has a Windows operating system, navigate to **`c:\Windows\Temp`** and delete all numbered **`_istmp`** directories.
3. If the target system has a Windows operating system:
   a. Navigate to `C:\Documents and Settings\<install_user_name>\Local Settings\Temp`
   b. Delete all `ismpXXX` and `LREXXX.tmp` directories.
4. Restart the target system.

Uninstalling Avaya Agent

Note:
The IC agent application uninstaller does not always remove all entries to the Windows registry. The remaining entries in the Windows Registry will not block functionality for other applications on the system.

To uninstall Avaya Agent:

1. Close all IC applications on the target system.
2. In the Windows Control Panel:
   a. Open **Add/ Remove Programs**.
   b. Select **Avaya IC** 7.3 **(Rich Client)**.
   c. Select **Change/Remove** to start the IC Uninstaller.

   Follow the prompts in the IC Uninstaller to uninstall IC services, delete registry settings, and remove files that are not in use.
3. In the Windows Control Panel, delete the IC environment variable:
   a. Double-click **System**.
   b. On the **Advanced** tab, select **Environment Variables**.
   c. Select the IC environment variable in the **System Variables** box.
   d. Click **Delete**.
   e. Click **Ok**.

4. For the `...\Backup` directory that was created by the agent installer:
   a. Review the files in the directory.
   b. Confirm that the System32 files are not required by another application.
   c. Restore any files required by another application.
   d. Delete the directory.
5. Delete any remaining folders and files in the *IC_INSTALL_DIR*`\IC73\` directory.
6. Delete all shortcuts that you added to the desktop.

Uninstalling Avaya Agent Web Client

You must completely remove the Avaya Agent Web Client software and settings if you need to re-install the software.

This section includes the following topics:

1. Uninstalling the Avaya Agent Web Client application on page 500
2. Uninstalling Avaya Agent Web Client Connector on page 500

Before you begin

Before you uninstall Avaya Agent Web Client, perform the following steps:

1. Ensure that all the agents are logged out.
2. Stop the Web Client Connector. For more information, see Starting and stopping Avaya Agent Web Client on page 463.

Uninstalling the Avaya Agent Web Client application

1. Browse to the *IC_INSTALL_DIR*`/IC73/tomcat/webapps` location and delete the `avaya` folder.
2. Browse to the *IC_INSTALL_DIR*`/IC73/tomcat/war` folder and delete the `webclient.war` file.

Uninstalling Avaya Agent Web Client Connector

Follow the instructions in Uninstalling IC on page 496 to uninstall the Avaya Agent Web Client Connector.

Appendix A: Configuring a localized version

To configure a localized version of IC, perform the steps in the following topics during the installation:

- About localized versions of IC on page 503
- About the NLS Lang setting for Oracle on page 503
- Enabling Database Designer for localization on page 505
- Configuring Avaya Agent for a supported language on page 507
- Configuring IC for multiple languages on page 508
- Importing localized seed data on page 509
- Configuring the website for supported languages on page 509
- Setting language properties for agents on page 510
- Localizing string table messages on page 512
- Configuring a Notification server for alternate email encodings on page 513
- Configuring an HTTP Connector server for Traditional Chinese on page 514
- Configuring an HTTP Connector server for Russian on page 514
- Configuring the Customer HTML Chat Client for Japanese IMEs (optional) on page 515

About localized versions of IC

The localized version of an IC release allows IC agent desktop applications to run in the supported languages for that release.

Typically, the localized version is delivered thirty days after the English release. However, for some releases, the localized version is delivered with the English release.

Where necessary, the topics in this section provide instructions for both types of delivery.

The following are known limitations of localization in IC:

Menu items may not be localized: Some menu items in Avaya IC applications are not completely localized. These items display in English. For example, you may see English text in some secondary built in forms and menu items, and on **OK** and **Cancel** buttons on some dialog boxes.

Accelerator keys do not work in Russian: Accelerator keys do not work for Web Agent in Russian. Ensure agents who work with Web Agent in Russian are aware that accelerator keys do not work.

For a list of the languages supported for a specific release, see *Avaya IC Installation Planning and Prerequisites*.

About the NLS Lang setting for Oracle

If your IC system includes an Oracle database, you must specify the NLS Lang property on the **Initial Configuration** tab of the Configuration Tool when you configure a primary or secondary server environment. The Configuration Tool automatically adjusts these settings when you provide the NLS_LANG parameter in the **Initial Configuration** tab.

Note:
The NLS Lang setting must match the value used to create the Oracle database. This value must include UTF8, because IC requires a UTF8 database.

This section includes the following topics:

- About the NLS Lang property on page 504
- Where Oracle specifies the NLS Lang property on page 504
- Cautions for the NLS Lang property on page 504
- NLS Lang settings for supported languages on page 504

For more information, see the Oracle documentation.

About the NLS Lang property

Oracle uses National Language Support (NLS LANG) values to set up language-specific databases. The character set part of the NLS_LANG parameter specifies the character set used by the Data server.

Where Oracle specifies the NLS Lang property

NLS_LANG is specified as an environment variable.

NLS_LANG is set in the registry under the following:

HKEY_LOCAL_MACHINE > SOFTWARE > ORACLE > HOMEn

Cautions for the NLS Lang property

Do not use abbreviations in the NLS LANG parameter. For example, do not use "US" to designate American English. You must use AMERICAN_AMERICA.UTF8.

The character set in the NLS LANG parameter must match the character set of your Oracle database. If these character sets are different, strange character conversions and string truncations may result.

NLS Lang settings for supported languages

The following table includes the NLS Lang settings for the languages supported in this IC release.

Language	NLS Lang Setting
English	AMERICAN_AMERICA.UTF8
Spanish	SPANISH_SPAIN.UTF8
German	GERMAN_GERMANY.UTF8
French	FRENCH_FRANCE.UTF8
Italian	ITALIAN_ITALY.UTF8
Portuguese	BRAZILIAN PORTUGUESE_BRAZIL.UTF8
Simplified Chinese	SIMPLIFIED CHINESE_CHINA.UTF8

Language	NLS Lang Setting
Korean	KOREAN_KOREA.UTF8
Japanese	JAPANESE_JAPAN.UTF8
Thai	THAI_THAILAND.UTF8
Traditional Chinese	TRADITIONAL CHINESE_TAIWAN.UTF8
Russian	RUSSIAN_CIS.UTF8

Enabling Database Designer for localization

To use Database Designer with languages other than English, you must add a Localization section to the Database Designer INI file (`qdesigner.ini`). This section identifies the character encoding that you are using for translations in your locale.

When you open an ADL file for localization, your Database Designer INI file must contain a Localization section with character encoding that matches the language in the localized design.

The Localization section includes the following:

- ISO-639-1 (alpha 2) two letter language abbreviations
- Character encoding used in the output generated by Database Designer

The two letter language abbreviation also identifies the language in all language-specific files.

Important:
You must host Database Designer on a system with an operating system that supports the target encoding. For example, you can use a localized version of Windows, or set the default system locale to the correct region in the **Regional Options** section of the Windows Control Panel.

To enable localization in Database Designer:

1. With Database Designer closed, open the Database Designer INI file (qdesigner.ini) in Notepad or another text editor.

   The Database Designer INI file is installed in the Windows directory. For example, in the systems using Windows, the Windows directory is typically `C:\Windows`.

2. Add a Localization section at the end of the INI file, including values for TargetLanguage and TargetEncoding fields to match the required locale using the information in the following table:

Language	Language Code	Localization Section Update

English	en	`[Localization]`
		`;English`
		`TargetLanguage=en`
		`TargetEncoding=windows-1252`

Spanish	es	`[Localization]`
		`;Spanish`
		`TargetLanguage=es`
		`TargetEncoding=windows-1252`

German	de	`[Localization]`
		`;German`
		`TargetLanguage=de`
		`TargetEncoding=windows-1252`

French	fr	`[Localization]`
		`;French`
		`TargetLanguage=fr`
		`TargetEncoding=windows-1252`

Italian	it	`[Localization]`
		`;Italian`
		`TargetLanguage=it`
		`TargetEncoding=windows-1252`

Portuguese	pt	`[Localization]`
		`;Portuguese`
		`TargetLanguage=pt`
		`TargetEncoding=windows-1252`

Simplified Chinese	zh	`[Localization]`
		`;Simplified Chinese`
		`TargetLanguage=zh`
		`TargetEncoding=gb2312`

Korean	ko	`[Localization]`
		`;Korean`
		`TargetLanguage=ko`
		`TargetEncoding=korean`

Language	Language Code	Localization Section Update
Japanese	ja	[Localization] ;Japanese TargetLanguage=ja TargetEncoding=shift_jis
Thai	th	[Localization] ;Thai TargetLanguage=th TargetEncoding=windows-874
Traditional Chinese	zt	[Localization] ;Traditional Chinese TargetLanguage=zt TargetEncoding=Big5
Russian	ru	[Localization] ;Russian TargetLanguage=ru TargetEncoding=windows-1251

3. Save the INI file.
4. Close the text editor.

Configuring Avaya Agent for a supported language

You do not need to perform these steps for Avaya Agent Web Client. Perform these steps for only Avaya Agent.

To configure Avaya Agent for a supported non-English language:

1. When you generate your Interaction Center data source (as discussed in Generating the Interaction Center application on page 151):
   a. Check the **Avaya Agent Layout** box and select an Avaya Agent Layout for the appropriate language.
   b. Check the **EDU Layout** box and select an EDU Layout for the appropriate language.

      If you do not know the directory path, select the **Ellipsis** (**…**) button and navigate to the directory.
2. To create and run the Agent Installer, follow the instructions in Creating installation files for agent applications on page 398.
3. Install the Language Interface Pack on agent system.

4. Apply the regional settings configuration. You might require to restart the computer.

Configuring IC for multiple languages

If your IC system requires that Avaya Agent or Avaya Agent Web Client run in multiple languages, you must store the messages for each language in the database. Perform these steps after you generate the Interaction Center data source for the first language.

To configure Avaya Agent for multiple languages:

1. Close Database Designer if you have it open.
2. Update the **[Localization]** section of the Database Designer INI file for the language.

   For more information, see Enabling Database Designer for localization on page 505.
3. In Database Designer, open the CCQ ADL file.
4. Select **File** > **Generate Windows Application**.
5. In the **Generate Windows Application** dialog box:
   a. Check the **Messages** box only.
   b. Check the **Avaya Agent Layout** box and select an Avaya Agent Layout for the appropriate language.
   c. Check the **EDU Layout** box and select an EDU Layout for the appropriate language.

      To find the path, select the **Ellipsis** (**…**) button and navigate to the directory.
   d. Select **interaction_center** from the **Name** list.
   e. Type the path for the directory where you want Database Designer to store the application files.

      For example, type `AVAYA_IC73_HOME\apps`.

      To find the path, select the **Ellipsis** (**…**) button and navigate to the directory.
   f. From the **DB Connection Set** drop-down list, select **defaultDBConnectionSet**.

g. If the fields in the following table do not have entries, re-enter your IC Manager account and password.

Field	Recommended entry
Login Id	Type your IC Manager login ID. **Note:** Do not use your DBA login ID and password.
Password	Type your password.

h. Click **Ok**.

Repeat these steps for each additional language.

Importing localized seed data

The localized seed data allows your IC system to have localized interfaces for the website. You perform these steps on the system that hosts Database Designer.

To install the localized seed data:

1. In Notepad or another text editor, open the following file: *IC_INSTALL_DIR*\IC73\design\CallCenterQ\data\L10N\seed_L10N.cfg.
2. Verify that the **DestinationPasswd** field has the correct password for the Admin account.
3. Save the `seed_L10N.cfg` file.
4. Open a command window.
5. Navigate to *IC_INSTALL_DIR*\IC73\design\CallCenterQ\data\L10N.
6. Run the following file to import the localized seed data: `import_seed_L10N.bat`

Configuring the website for supported languages

To configure your website for supported languages:

1. In IC Manager, select **Services** > **MultiTenancy Administration**.
2. Select **Define Languages** from the **Tenants Admin** menu.
3. In the **Properties** box:

a. Select a language code.

   For both Simplified Chinese and Traditional Chinese, select **zh**.

b. Assign a country/region code:

   - For Traditional Chinese, select **TW**.
   - For all other supported languages, leave the country/region code blank.

c. Type a default description.

d. Type a default display name.

e. Select **Add Language**.

If IC cannot find a property for a supported language, IC will use the default language. English is always the default language for the default tenant.

Setting language properties for agents

When you configure the language for an agent, you specify the language that the agent desktop applications use. You must set this property for all agents who work with an agent desktop language other than English.

Note:
Web Agent obtains the language setting from Avaya Agent. You do not need to configure the language for Web Agent separately.

To configure the agent language property for agents:

1. In IC Manager, select **Tools** > **Groups**.
2. Select the **Properties** tab.
3. Select the **IC** node in the left pane.
4. In the **Sections** list, select **Agent**.
5. Double-click the **UILanguage** property.
6. In the **Edit Property UILanguage** dialog box:
   a. From the **Property Value** drop-down list, select one of the values in the following table:

Value	Language
de	German
en	English

Value	Language
es	Spanish
fr	French
it	Italian
ja	Japanese
ko	Korean
pt	Portuguese
ru	Russian
th	Thai
zh	Simplified Chinese
zt	Traditional Chinese **Note:** zt is a non-standard two letter language code that certain components of IC use differentiate between Traditional Chinese and Simplified Chinese.

b. Click **Ok**.

7. For languages that have regional variations of a particular language, such as Simplified Chinese and Traditional Chinese:

   a. Double-click the **UICountryOrRegion** property.

   b. From the **Property Value** drop-down list, select one of the values in the following table.

Value	Language
CN	China (Simplified Chinese)
TW	Taiwan (Traditional Chinese)

   Setting the **UICountryOrRegion** property also allows for regional differences in the date and time formats. For more information about how to customize Avaya Agent Web Client for regional differences, see *Avaya Agent Web Client Customization*.

   c. Click **Ok**.

8. Click **Ok**.

Localizing string table messages

You can use the **Localization** node in Database Designer to localize messages in the string table. For more information, see *IC Database Designer Application Reference*.

This section includes the following topics:

- Translating string table messages on page 512
- Deleting string table messages on page 512

Translating string table messages

To translate string table messages:

1. Under the **Localization** placeholder, select **String Table** in the tree view.

   The String Table **Properties** tab opens and displays all available string table messages.
2. In the String Table **Properties** tab, select the message to be translated.
3. Select the message text in the **String Text** column.
4. Delete the message text and type in the translation.
5. Select **File** > **Save** to save the ADL file with the localized string table entries and generate the ALM file.

Deleting string table messages

If you delete a string table message that is connected to a form, the Avaya Business Application is not able to display the message to the user.

To delete a string table message:

1. In the String Table **Properties** tab, select the message to be deleted.
2. Select **Delete**.

Configuring a Notification server for alternate email encodings

The Notification server uses a default Microsoft Windows codepage value for the outgoing email charset. You can override this value on the **Configuration** tab of the Notification server in IC Manager.

For example, if you want to use an alternate email encoding for a supported languages, such as iso-2022-jp instead of Windows-932 (Shift-JIS) for Japanese, you need to configure the Notification server to accept the alternate email encoding.

To configure a Notification server for alternate email encodings:

1. In IC Manager, double-click the HTTP Connector server in the lists of servers.
2. Select the **Configuration** tab.
3. Select **New**.
4. In the **CTI Type Editor** dialog box:
   a. Complete the fields as shown in the following table:

Field	Recommended entry
CTI Type	Couple
Name	charset This field is case-sensitive.
Value	*EmailCharset* where EmailCharset is the character set for the alternate email encoding. For example, type **`iso-2022-jp`** for Japanese.

   b. Click **Ok**.
5. Click **Ok**.
6. Stop and restart the Notification server.

Configuring an HTTP Connector server for Traditional Chinese

To configure an HTTP Connector server for Traditional Chinese:

1. In IC Manager, double-click the HTTP Connector server in the lists of servers.
2. Select the **Configuration** tab.
3. Select **New**.
4. In the **CTI Type Editor** dialog box:
   a. Complete the fields as shown in the following table:

Field	Recommended entry
CTI Type	Couple
Name	charsetmap This field is case-sensitive.
Value	Big5:Big5

   b. Click **Ok**.
5. Click **Ok**.
6. Stop and restart the HTTP Connector server.

Configuring an HTTP Connector server for Russian

To configure an HTTP Connector Server for Russian:

1. In IC Manager, double-click the HTTP Connector server in the lists of servers.
2. Select the **Configuration** tab.
3. Select **New**.

4. In the **CTI Type Editor** dialog box:
   a. Complete the fields as shown in the following table:

Field	Recommended entry
CTI Type	Couple
Name	charsetmap This field is case-sensitive.
Value	windows-1251:cp1251

   b. Click **Ok**.
5. Click **Ok**.
6. Stop and restart the HTTP Connector server.

Configuring the Customer HTML Chat Client for Japanese IMEs (optional)

Some Japanese Input Method Editors (IMEs) use the **Enter** key to select characters. If a website customer uses one of these IMEs, the Customer HTML Chat Client may respond to the **Enter** key and send the message prematurely. You can configure the Customer HTML Chat Client not to automatically send a message when a customer presses the **Enter** key.

If you disable Send on Enter, the website customer must select **Send** in the Customer HTML Chat Client to send a chat message to an agent.

To configure the Customer HTML Chat Client for Japanese IMEs:

1. In IC Manager, select **Services** > **MultiTenancy Administration**.
2. Select **Tenant Properties** in the **Tenant Admin** menu.
3. Select the tenant you want to customize from the **Select a Tenant** drop-down list.
4. Select **Customize Tenant**.
5. In the **Customize Tenant** page:
   a. Select **Japanese** from the **Select Language** drop-down list at the top of the page.
   b. Select **chat**.
   c. Scroll down to the **chat.htmlclient.entry.sendonenter** property.
   d. Change the value of this property to 0.
   e. Select **Update Data** at the bottom of the page.

Appendix B: Changing default service ports

Changing default service ports

This section includes the following topics:

- Changing default ICM service ports on page 516
- Changing default service ports for servers on page 518

Changing default ICM service ports

You can change some ICM service ports as described in the following topics:

- Changing ICM tunnel port on website on page 516
- Changing ICM tunnel port on CSPortal on page 517
- Changing CIRS servlet port on page 517

Changing ICM tunnel port on website

To change the ICM tunnel port on website:

1. On the system that hosts the ICM server, open the following file in a text editor:
   IC_INSTALL_DIR\IC73\comp\website\WEB-INF\web.xml
2. In the section for the HTMLClient servlet, add a new port parameter with the value:

```
<servlet>
    <servlet-name>HTMLClient</servlet-name>
    <servlet-class>com.avaya.icm.htmlclient.HCServlet</
servlet-class>
   <init-param>
<param-name>port</param-name>
<param-value>"new port number"</param-value>
</init-param>
    <load-on-startup>4</load-on-startup>
  </servlet>
```

3. Save the `web.xml` file.
4. Restart the website.

Changing ICM tunnel port on CSPortal

To change the ICM tunnel port on CSPortal:

1. On the system that hosts the ICM server, open the following file in a text editor: `IC_INSTALL_DIR\IC73\comp\csportal\WEB-INF\web.xml`
2. In the section for the HTMLClient servlet, add a new port parameter with the value:

```
<servlet>
    <servlet-name>HTMLClient</servlet-name>
    <servlet-class>com.avaya.icm.htmlclient.CSPHCServlet</
servlet-class>
   <init-param>
<param-name>port</param-name>
<param-value>"new port number"</param-value>
</init-param>
    <load-on-startup>4</load-on-startup>
  </servlet>
```

3. Save the `web.xml` file.
4. Restart CSPortal.

Changing CIRS servlet port

To change the CIRS servlet port:

1. On the primary system that hosts the ICM server and the Website, open the following file in a text editor: *`IC_INSTALL_DIR`*`\IC73\comp\website\WEB-INF\web.xml`.
2. In the section for the CIRS servlet, add a new parameter with the value in the following table:

Parameter	Value
port	new port number

3. Save the `web.xml` file.
4. Restart the website.

Changing default service ports for servers

You can change the default service ports, if required, as shown in the following topics:

- Changing the service port for the WebACD server on page 518
- Changing the service port for the ComHub server on page 518
- Changing the service port for the Paging server on page 519
- Changing the service port for the Attribute server on page 519

Changing the service port for the WebACD server

For more information about the WebACD server, see Creating the WebACD server on page 196.

To change the service port for the WebACD server:

1. In IC Manager, update the WebACD server configuration:
   a. Double-click the WebACD server in the list of servers.
   b. Click the **WACD** tab.
   c. Change the port number in the **Service Port** field.
2. In Notepad or another text editor, open the Webadmin.cfg file, and change the service port property to the new port number.

Changing the service port for the ComHub server

For more information about the ComHub server, see Creating the ComHub server on page 202.

To change the service port for the ComHub server:

1. In IC Manager, update the ComHub server configuration:
   a. Double-click the ComHub server in the list of servers.
   b. Click the **ComHub** tab.
   c. Change the port number in the **Service Port** field.
2. In IC Manager, update the `masterserverport` property of the WebACD server:
   a. In the list of servers, double-click the associated WebACD server in the same domain.
   b. Click the **WACD** tab.
   c. Change the value of the **Comhub Port** field to the new port.
3. In IC Manager, update the Paging server configuration:
   a. In the list servers, double-click the Paging server.

b. Click the **Paging** tab.
c. Right-click an empty area in the tab and select the **Show Advanced Properties** box.
d. Change the value of the **Comhub Port** field to the new port.

Changing the service port for the Paging server

For more information about the Paging server, see Creating the Paging server on page 204.

To change the service port for the Paging server:

1. In IC Manager, update the Paging server configuration
   a. Double-click the Paging server in the list of servers.
   b. Click the **Paging** tab.
   c. Change the port number in the **Service Port** field.
   d. Click **Apply**.
   e. Click **OK**.

Changing the service port for the Attribute server

For more information about the Attribute server, see Creating the Attribute server on page 200.

To change the service port for the Attribute server:

1. In IC Manager, update the Attribute server configuration:
   a. Double-click the Attribute server in the list of servers.
   b. Click the **Attribute** tab.
   c. Change the port number in the **Port** field.
2. In Notepad or another text editor, open the `datawake.cfg` file, and change the service port property to the new port number.

Appendix C: Configuration Tool advanced properties

On the **Web** tab, you can find advanced properties that include the following properties for the Java Virtual Machine:

- Initial heap size and maximum heap size
- Stack size

Tip:
Configure the advanced properties only if you expect a high volume of contacts or access to the Web application. For example, configure the advanced properties for the website and the ICM server if you expect a high volume of chat contacts from the customer website. For information about performance and contact volume, see the benchmarking information available through an Avaya representative.

This section describes the advanced properties on the **Web** tab and how to access those properties. The topics include:

- Format of the advanced properties on page 521
- Accessing the advanced properties on page 520
- Advanced properties on page 522
- Using the recommended settings for the advanced properties on page 523

Accessing the advanced properties

To access the advanced properties on the **Web** tab of the Configuration Tool:

1. Right-click in an empty space on the **Web** tab.
2. Select the **Show Advanced Properties** check box.

Format of the advanced properties

The advanced properties use the following format:

`-<initial_Java_heap> -<maximum_Java_heap>`

where:

Format	Property	Description
initial_Java_heap	-Xms	Sets the initial Java heap size for the Tomcat application.
	--JvmMs	Sets the initial Java heap size for the Tomcat service.
maximum_Java_heap	-Xmx	Sets the maximum Java heap size for the Tomcat application.
	--JvmMx	Sets the maximum Java heap size for the Tomcat service.

Advanced properties

The following table describes the fields on the **Web** tab for advanced properties.

Field	Description	Default value
Tomcat Setup	The Multiple option creates a separate Tomcat server for each Web application. Choose Multiple if the system hosts more than one Web application, and you want to start and stop all Web applications separately.	Multiple

Web License Manager JVM Options	Available only when you select **Configure Web License Manager**.
	Entries must use the following format:
	-<*min_heap*>
	-<*max_heap*>
	-<stack_size>
		`--JvmMs 32 --JvmMx 64 --JvmSs 96`
		`-Xms32m -Xmx64m -Xss96k`
		`-Xms32m -Xmx64m -Xss96k`
		Note: To increase the license capacity, you must increase the minimum and maximum heap size as mentioned below:
		`--JvmMs 256 --JvmMx 512 --JvmSs 96`
		`-Xms256m -Xmx512m -Xss96k`
		`-Xms256m -Xmx512m -Xss96k`

Email Template Administration JVM Options	Available only when you select **Configure Email Template Administration**.
	Entries must use the following format:
	-<*min_heap*>
	-<*max_heap*>
		`--JvmMs 32 --JvmMx 64`
		`-Xms32m -Xmx64m`
		`-Xms32m -Xmx64m`

Website JVM Options	Available only when you select **Configure Website**.
	Entries must use the following format:
	-<*min_heap*>
	-<*max_heap*>
		`--JvmMs 64 --JvmMx 256`
		`-Xms64m -Xmx256m`
		`-Xms64m -Xmx256m`
		Note: To increase the chat handling capacity of csportal and public website, you must increase the minimum and maximum heap size as mentioned below:
		`--JvmMs 256 --JvmMx 1024`

Field	Description	Default value
ICM JVM Options	Available only on Windows, when you select **ICM Service**. Entries must use the following format: -<*min_heap*> -<*max_heap*>	All Platforms: `-Xms64m -Xmx256m`
CIRS JVM Options	Available only when you select **CIRS Service**. Entries must use the following format: -<*min_heap*> -<*max_heap*>	All Platforms: `-Xms32m -Xmx64m`

Using the recommended settings for the advanced properties

The recommended tuning parameters in *Interaction Center Administration Guide* also includes some recommended settings for the advanced properties.

After you install the development IC system as described in this document:

1. Review the tuning parameters in *Interaction Center Administration Guide*.
2. Verify the expected contact volume in the production system.
3. Test the recommended settings for the tuning parameters to find the optimal settings for the production system.

Index

Symbols

.NET client, running 480

A

accessing, advanced properties 520
accounts
Admin 79
agent 378
creating 77, 80
customer 355
disabled 355
email 354
human users 80
icmbridge 80
Java Application Bridge 449, 473
non-human users 78
passwords 78
Web Services Bridge 486
website 79

ACDname 173
adding
ICM servers to ICM Bridge 286
knowledge base 372
routing hints 234, 350
Address Book
configuring agents 391, 394
configuring Workflow server 395
ADL file 132, 135
Admin account 79
administration website
configuring 277
setting up 277
Web application 277
administrative accounts
creating 80
human users 80
non-human users 78
Administrative Content Analyzer server 369
administrator login 29
ADU server
stopping 107
updating 85
advanced properties
accessing 520
Configuration Tool 520
recommended settings 523
Advocate
see Business Advocate
agent accounts
Avaya Agent 386
Avaya Agent Web Client 390
cautions 376
Client SDK 392
creating 378
Java Application Bridge 449, 473
Web Services Bridge 486
agent applications
automatic updates 406
installation files 399
agent installer
copying vesp.imp 403
creating 402
network drive 405
preparing for installation 404
testing 404
agent properties 392
AgentAlreadyRunningMsg 438
AgentDesktopCtr.ini 437

agents
configuring for Address Book 391, 394
configuring for Avaya Agent 386
configuring for Avaya Agent Web Client 390
configuring for Unified Agent Directory 388
creating 376, 378
home directory 387
installation 398
installing applications 374, 398
properties 392
properties for Avaya Agent 387
properties for Avaya Agent Web Client 390
setting properties 384
updating version.html 407
Web Scheduled Callback 257
working directory 390, 392, 447
agentsearch.update_searchresult 396
AIX
changing ownership 463
configuring full-text searches 254
installing
Avaya Agent Web Client connector 41
Server SDK 63
servers 41
installing Avaya Agent Web Client connector 41
installing Client SDK 41
prerequisites 31

starting Client SDK server ... 119, 478
starting Web Services server ... 119, 492
stopping Client SDK server ... 120, 478
stopping Web Services server ... 120, 492
updating full text index ... 256
updating index ... 256
windowing environment ... 31
analyze flow ... 331
applications
IC Repository ... 142
Interaction Center ... 151
AskForExitConformation ... 439
associations
Email Management ... 343
Telephony ... 187
Web Management ... 230
Attribute server
about ... 196
adding ICM servers to ICM Bridge ... 286
changing service port ... 519
creating ... 200
ICM bridge ... 202
Web configuration ... 211, 220, 224
automatic updates
configuring ... 406
disabling ... 408
version.html ... 407
autostart
CIRS server on UNIX ... 116, 118
IBM HTTP server ... 119
ICM server on UNIX ... 116, 118
Oracle iPlanet Server ... 116
services ... 114
Tomcat applications on UNIX ... 117, 120
Avaya Agent
agent properties ... 387
automatic updates ... 406
Citrix integration ... 419
configuring agents ... 386
documents ... 26
home directory ... 387
installation files ... 399
Internet Explorer ... 399
internet options ... 399
modifying layout ... 144
site preparation wizard ... 402
Web Scheduled Callback ... 258
Avaya Agent Web Client
Address Book ... 391
administrator privileges ... 446
agent properties ... 390
application
redeploying ... 468
configuring ... 444, 460
configuring agents ... 390
configuring SSL ... 466
documents ... 26
installing connector
AIX ... 41
Solaris ... 39
Windows ... 37
Internet Explorer ... 445
internet options ... 445
Java Application Bridge ... 449, 451
JRE version ... 446
ownership for UNIX ... 463
pop-up blockers ... 446
prerequisites ... 445
proxy server settings ... 446
re-installing ... 458
testing ... 466
UNC to UNIX mapping ... 454
WAR file ... 462
Web Scheduled Callback ... 258
working directory ... 390, 447
Avaya Computer Telephony for IC
see Telephony
Avaya IC ORB Service ... 111

B

base, knowledge ... 372
BasicStartAgent.htm ... 434
blender flows ... 82
Blender server, creating ... 98
bridge, Web Services ... 485
building
Business Advocate databases ... 54, 58
CCQ database ... 144
IC Repository ... 135
Business Advocate
creating environment ... 53
database schema ... 54, 58
documents ... 27
nethome ... 53, 58, 60
Nethome directory ... 52
permissions for ECB ... 61
prerequisites ... 52
requirements ... 51

C

calendar, Web Scheduled Callback ... 258
callback.checkcallbacktime ... 260
callback.contactcenterclosetime ... 260
callback.contactcenteropentime ... 260
CallCenterQ database
see CCQ database
cautions
agent accounts ... 376

Avaya Agent installation ... 399
Data server ... 124
Design & Administration Tools ... 34
server installation ... 32, 33
Web Scheduled Callback ... 257
CCQ database
building ... 144
connection set ... 150
creating ... 143, 150
database connection ... 144
ccq.adl ... 133
ccqDBConnection ... 144
CDL file ... 144
Central Internet Routing Service ... 240
changing
ownership for UNIX ... 49, 463
service ports ... 518
Web License Manager password ... 168
channels
email ... 326
Email Management ... 343
servers ... 196, 329
Telephony ... 187
voice ... 172
web ... 194
Web Management ... 230
character encoding ... 505
chat
RONA ... 194
Workflow server ... 229
ChatLoginServer ... 227, 279
ChatLoginServerPort ... 228
ChatLoginServerProtocol ... 228
ChatLoginServerWebsite ... 227, 279
CIRS server
additional ICM ... 282, 284
autostart on UNIX ... 116, 118
configuring ... 240
configuring for website ... 285
start on UNIX ... 116, 118
stop on UNIX ... 116, 118
CIRS service ... 211, 220, 225
Citrix integration
configuring ... 419
configuring INI file ... 432
executable tool
components ... 437
configuring ... 436
INI file ... 437
installing ... 437
multiple Citrix servers ... 440
installing applications ... 420
limitations ... 420
location of files ... 431
publishing applications ... 419
seamless window ... 420
sequence for Avaya tools ... 440
Web browser tool
components ... 434
configuring ... 433
installing ... 434
multiple Citrix servers ... 436
updating HTML page ... 435
CitrixClientURL ... 435, 437
client login flow ... 100
Client SDK
creating environment ... 476
deploying ... 470
documents ... 26
files ... 472
installing ... 471
AIX ... 41
Solaris ... 39
Windows ... 37
Java Application Bridge ... 473
prerequisites ... 470
secondary ORB server environment ... 472
SSL ... 492
Web Scheduled Callback ... 258
Client SDK server
starting ... 114, 117, 119, 477, 478
stopping ... 117, 120, 477, 478
ClientBarHight ... 438
ClientBarWidth ... 438
CM
Telephony server ... 175
TSQS server ... 184
ComHub server
about ... 202
changing service port ... 518
creating ... 202
Communication Manager
TS ... 175
TSQS server ... 184
components
executable tool for Citrix ... 437
Web browser tool for Citrix ... 434
Configuration Tool
administration website ... 277
Business Advocate ... 53
customer Website ... 279
Email Template Administration ... 333
initial configuration ... 45, 47
SDK server ... 476
Web ... 206
configuring
ACD name ... 173
additional ICM server ... 282, 283
administration website ... 277
agents for Avaya Agent ... 386

agents for Avaya Agent Web Client....390
agents for Unified Agent Directory....388
Avaya Agent Web Client....444, 460
Business Advocate....53
CCQ connection set....150
CCQ database connection....144
Client SDK....470
CM TS....175
Content Analyzer....368
core servers....72, 83
customer Website....279
Data server....123, 124
Data server for DB2....130
Data server for Oracle....127
Data server for SQL Server....124
email accounts....354
Email Management....326
Email Template Administration....333, 353
executable tool for Citrix....436
FTSE....248
full-text searches on AIX....254
full-text searches on Solaris....251
full-text searches on Windows....248

home directory....387
HTTP Connector server....514
IC Email server....329
IC Repository connection set....139
IC Repository database connection....135
ICM server....237
independent ICM....285
License server....167
media channels....195, 382
Notification server....513
primary ICM for additional ICM....282
primary servers....45
secondary servers....47
send on enter for Japanese IMEs....515
servers....196
SSL for Avaya Agent Web Client....466
Telephony....172
UNC to UNIX mapping....456
Web browser tool for Citrix....433
Web Management....194
Web Management services....206
Web Scheduled Callback....257
Web Services....484, 490
WebACD server....352
Website....206
website....241
Website for Web Scheduled Callback....259
Workflow server....186, 229, 342
Workflow server for agents....395
working directory....390, 392
connection sets
CCQ database....150
IC Repository....139
connections
CCQ database....144
IC Repository....135
console layout....144
Content Analyzer
adding knowledge base....372
Administrative server....369
configuring....368
knowledge base....372
Operations server....370
copying vesp.imp....403
core servers
configuring....72, 83
recommended settings....85
CPU resources, IC Manager....34
creating
accounts....77, 449, 473, 486
Administrative Content Analyzer server....369
agent accounts....378
agent installation files....399
agent installation instructions....405
agent installer....402

agents....376, 378, 392
Attribute server....200
Blender server....98
Business Advocate environment....53
CCQ database....150
ComHub server....202
domains....76
EDU server....91
email status....367
HTTP Connector server....100
IC Email server....327, 329
IC Repository....140
Java Application Bridge....451
knowledge base....372
License server....167
Notification server....103
Operations Content Analyzer server....370
Paging server....204
Report server....93
routing hints
Email Management....350
Telephony....191
Web Management....234
SDK server environment....476
secondary Directory server....90
sites....73
Telephony server....174
TSQS server....183
Web Scheduled Callback server....258
Web Services Bridge....487
WebACD server....196
Workflow server....186, 229, 342

creating Java Application Bridge....474
CTI
See Telephony
customer account....355
Customer HTML Chat Client, Japanese....515
customer Website
configuring....279
setting up separate....279
Web application....279
customizing Avaya IC....26

D

data models....26
Data server
cautions....124
configuring....123
DB2....130
Oracle....127
primary....124
secondary....132
SQL Server....124
data sources
Interaction Center....151
repository....142
understanding....132
Database Designer....135
Database Host....221, 226
Database Login....212, 221, 225
Database Password....212, 221, 226
database system....124
databases
Business Advocate....54, 58
CCQ....143
connection sets....139, 150
connections....135, 144
documents....26
IC Repository....134
Repository....212, 221, 225
dataserver type/alias....136, 146
DataWake....200, 201
DB2
Data server....130
DB2 Instance....46, 48
qdb2sp library....123
DB2 Port....226
DB2DIR....254
deleting, string table messages....512
dependencies, servers....107
deploying
Avaya Agent Web Client....444, 460
Client SDK....470
Web Services....484
Design & Administration Tools
cautions....34
components....34
Database Designer....135
installing....37
systems....34
tips....34
directory
home....387
working....390
Directory server
routing hints....191, 234, 350
secondary....90
updating....142
directory, working....392
disabled accounts....355
DisableStartButtonAfterFirstClick....439
disabling automatic updates....408
display time
CCQ database....145
IC Repository....136
documentation....26
domains
administration....35
creating....76
failover....76
guidelines....75
IC Email server....327, 329
Java Application Bridge....452, 475
preconfigured....74
Web Services Bridge....488
DontStartMultipleInstancesOfAgent....435, 438
ds.ffd....91
DUStore server
stopping....107
updating....86

E

ECB, verifying permissions....61
EDU server
creating....91
stopping....107
EDUs
creating EDU server....91
email
RONA....326
Workflow server....342
Email Management
configuring....326
configuring WebACD server....352
configuring Workflow server....343
email accounts....354
email status....367
Email Template Administration....353
optional configurations....326
prerequisites....327

RONA 326
routing hints 350
Workflow server 342
workflows 348
Email server
see IC Email server
Email Template Administration
configuring Web application 333
email status 367
integrating 353
JVM Options 522

EmailLoginServer 354
EmailLoginServerPort 354
EmailLoginServerWebsite 354
EmailServer 354
EmailServerPort 354
enabling localization 505
environment
Business Advocate 53
primary ORB 45
secondary ORB 47
error messages
deleting 512
translating 512
Event Collector Bridge, permissions 61
executable tool
AgentAlreadyRunningMsg 438
AskForExitConformation 439
caption properties 439
CitrixClientURL 437
ClientBarHight 438
ClientBarWidth 438
components 437
configuring 436
DisableStartButtonAfterFirstClick 439
DontStartMultipleInstancesOfAgent 438
INI file 437
installing 437
MaximizeWindowOnLanchedAppExit 439
MinimizeWindowOnLanchedAppStart 439
multiple Citrix servers 440

F

failover, domains 76
flows
Email Management 348
loading 190
sample 82
system 82
Telephony 189
Web Management 232
flush 127, 129, 131
FTSE, configuring 248

G

generating
IC Repository application 142
Interaction Center application 151
guidelines
additional ICM server 281
domains 75
server naming 84
Web Scheduled Callback 258

H

Heap size 520
home directory 387
HTTP Connector server
creating 100
Traditional Chinese 514
human users
administrative accounts 80
creating 80

I

IBM HTTP server
autostart 119
IC Data Source 212, 221, 225
IC Email server
about 329
creating 327, 329
failover 327, 329
guidelines 327, 329
IC Login 211, 220, 225
IC Manager
Admin account 79
CPU resources 34
logging in 35
multiple instances 35
stopping servers 112
Web Management administration pages 226
IC Password 211, 220, 225
IC Repository
building 135
connection set 139
creating 134, 140
data source 212, 221, 225
database connection 135
generating application 142
seed data 140
updating Directory server 142
ICEmail flows 82
ICM Bridge
adding ICM servers 286
enable 201

Comments on this document? infodev@avaya.com

ICM server
adding to ICM Bridge ... 286
additional ... 280
autostart on UNIX ... 116, 118
CIRS ... 240
CIRS for additional ICM ... 284
configuring ... 237
configuring additional ... 282, 283
configuring independent second ... 285
configuring primary for additional ICM ... 282
enabling CIRS ... 285
guidelines for additional ... 281
ICM bridge ... 202
icmbridge account ... 80
start on UNIX ... 115, 118
stop on UNIX ... 115, 118
ICM service ... 211, 220, 225
icmbridge account ... 80
idl ... 127, 129, 131
IMEs, Japanese ... 515
importing seed data ... 141, 151
index
updating on AIX ... 256
updating on Solaris ... 253
updating on Windows ... 249
INI file
configuring for Citrix ... 432
executable tool for Citrix ... 437
localization ... 505
initial configuration ... 45, 47
initialization flow ... 100
installer, agent ... 399, 402
installing
additional ICM servers ... 280
agent applications ... 374, 398
Avaya Agent Web Client connector
AIX ... 41
Solaris ... 39
Windows ... 37
Client SDK
AIX ... 41
Solaris ... 39
Windows ... 37
Client SDK components ... 471
DB2 qdb2sp library ... 123
Design & Administration Tools ... 37
executable tool for Citrix ... 437
license ... 165
on Citrix server ... 420
prerequisites ... 29
Server SDK
AIX ... 63
Solaris ... 63
Windows ... 63
servers ... 35
AIX ... 41
Solaris ... 39
Windows ... 37
Web browser tool for Citrix ... 434
Web Services components ... 485
integrating
Email Template Administration ... 353
Web Management administration pages ... 226
integration, Citrix ... 419
Interaction Center application ... 151
Internet Explorer, Avaya Agent Web Client ... 445

J

Japanese, send on enter ... 515
Java Application Bridge
agent account ... 449, 473
Avaya Agent Web Client ... 449
Client SDK ... 473
creating ... 451, 474
domain ... 452, 475
setting up ... 449, 473
starting ... 453, 476, 490
UNC to UNIX mapping ... 454
Java client, running ... 480
JavaAppBridge
see Java Application Bridge
JRE version ... 446

K

knowledge base ... 372

L

language abbreviations ... 505
language pack updates ... 406
layout, Avaya Agent ... 144
LCID abbreviations ... 505
license file ... 29
License server, configuring ... 167
licenses
installing ... 165
licensing
about ... 154
changing password ... 168
installing license ... 165
License server ... 167
prerequisites ... 154
limitations, Citrix integration ... 420
loading flows ... 190
locale ID ... 505
localization
character encoding ... 505

enabling 505
Japanese 515
language abbreviations 505
location
Citrix integration files 431
Logical Resource Manager
additional, database schema 58
first, database schema 54
login, administrator 29, 446

M

mailto 355
mapping, UNC to UNIX. 454
MaximizeWindowOnLanchedAppExit 439
maximum Heap size 520
maximum Stack size 520
media channels
agents 382
Email Management 326
prerequisites 195
Telephony 172
Web Management 194
migrating 64
MinimizeWindowOnLanchedAppStart 439
minimum Heap size 520
minimum Stack size 520
modifying
Avaya Agent layout 144
multiple database types 124
multiple Tomcat
starting on UNIX 116, 119
starting Website on UNIX 117, 119
stopping on UNIX 117, 119
stopping Website on UNIX 117, 120
multiple, IC Manager 35
MultiVantage TS 175

N

naming, servers 84
nethome 53, 58, 60
Nethome directory 52
network drive, agent installer 405
non-human users
administrative accounts 78
creating 80
Java Application Bridge 449, 473
Web Services Bridge 486
Notification server
alternate email encodings 513
creating 103

O

Operations Content Analyzer server 370, 372
Oracle
Data server 127
Oracle SID 46, 48
Oracle iPlanet Server
autostart 116
starting 116
stopping 116, 119
Oracle SID 46, 48, 221
ORACLE_HOME 251
ORB server
configuring 45
secondary 47, 472, 485
starting 110
stopping 110
orbsrv.exe 111
order, servers 107
outbound email flow 332

P

pa_admin 61
Paging server
about 204
changing service port 519
creating 204
passwords for accounts 78
permissions
agent installer 398
verifying for ECB 61
planning customization 26
point patch updates 406
pop-up blockers, Avaya Agent Web Client 446
ports
changing service ports 518
email server 354
preconfigured domains 74
preparing agent installer 404
prerequisites 29
agent applications 398
AIX 31
Avaya Agent Web Client 445
Business Advocate 52
Client SDK 470
core servers 72, 122, 304
Email Management 327
installation 29
JRE version 446
license 29
licenses 154
media channels 195
Solaris 31

Telephony 173
UNC to UNIX mapping 454
Web Scheduled Callback 257
Web Services 484
primary servers
creating environment 45
Data server 124
DB2 Instance 46, 48
Oracle SID 46, 48
Prompter flows 82
properties
agents 384, 392
Avaya Agent 387
Avaya Agent Web Client 390
Client SDK 392
home directory 387
working directory 390, 392
proxy server, Avaya Agent Web Client 446

Q

qdb2sp library 123
qntorbsrv.exe 111

R

Readme file 29
recommended settings
advanced properties 523
core servers 85
redeploying Avaya Agent Web Client 468
refresh
IC Manager 286
reinstalling
Avaya Agent Web Client 458
Avaya IC 64
Report server
creating 93
stopping 107
Repository
see IC Repository
Repository data source 212, 221, 225
repository.adl 133, 135
repositoryDBConnection 135
requirements
administrator login 29, 446
agent installer 398
Agent Site Preparation wizard 401
Business Advocate 51
core servers 72, 122, 304
data sources 132
Email Management 327
license 29
licenses 154
media channels 195
Telephony 173
UNC to UNIX mapping 454
Web Scheduled Callback 257
resource store, database schema 54
response library manager 333
Return on no answer
see RONA
rlmanager 333
RONA
Email Management 326
Telephony 172
Web Management 194
root, changing ownership 49, 463
routing hints 350
adding 234, 350
Telephony 191
Web Management 234
RoutingHint table 234, 350
running Agent Site Preparation wizard 402

S

Samba 454
sample workflows 82
SDK
Client SDK 37, 39, 41, 470
Server SDK 63
seamless window, Citrix 420
secondary servers
Client SDK 472
creating environment 47
Data server 132
ICM 280
Web Services 485
Secure Sockets Layer 466
security
passwords 78
seed data, IC Repository 140
seed.cfg 150
send on enter, Japanese 515
sequence for Avaya tools 440
Server SDK, installing 63
servers
administration 35
Administrative Content Analyzer 369
ADU 85
AIX 41
Attribute 196, 200, 286
Blender 98
Business Advocate 53
cautions and tips for installing 32, 33
Client SDK 114, 117, 119, 476, 477
ComHub 202
configuring 196
core 72, 83

Data....123
dependencies....107
documents....26
DUStore....86
EDU....91
HTTP Connector....100, 514
IC Email....327, 329
ICM....202, 237
installing....35
Java Application Bridge....451, 474
License....167
naming....84
Notification....103, 513
Operations Content Analyzer....370
Paging....204
recommended settings....85
reinstalling....64
Report....93
secondary Directory....90
Solaris....39
starting....107
starting primary....45
starting secondary....47
starting Telephony....185
startup dependencies....108
stopping....107
Telephony....174
TSQS server....183
Web Management....114
Web Scheduled Callback....258
Web Services....114, 117, 119, 491
Web Services Bridge....485, 487
WebACD....196, 352
Windows....37
Workflow
creating....94
Email Management....342
Telephony....186
transfers and conferences....395
Web Management....229
service pack updates....406
service ports
attribute server....519
changing....518
ComHub server....518
Paging server....519
WebACD server....518
services
starting on Windows....114
stopping on Windows....114
services, Web Management....206
setting agent properties....384
setting up
administration website....277
Data server....124
Java Application Bridge....449, 473
optional web configurations....194
separate customer Website....279
Web Services Bridge....485
sharing Nethome directory....52
ShowAgentsOnStartup....388, 389
ShowAgentState....389
ShowAllAgents....389
SID, Oracle....46, 48
site preparation wizard
Avaya Agent....402
sites, creating....73
SkillsSupport....389
Solaris
changing ownership....49, 463
configuring full-text searches....251
installing
Avaya Agent Web Client connector....39
Server SDK....63
servers....39
installing Avaya Agent Web Client connector....39
installing Client SDK....39
prerequisites....31
starting Client SDK server....117, 478
starting Web Services server....117, 491
stopping Client SDK server....117, 478
stopping Web Services server....117, 492
UNC to UNIX mapping....456
updating full text index....253
updating index....253
windowing environment....31
SQL Server, Data server....124
SSL
Tomcat....492
Stack size....520
starting
Business Advocate....53
CIRS server on UNIX....116, 118
Client SDK server....114, 117, 119, 476, 477, 478
ICM server on UNIX....115, 118
Java Application Bridge....453, 476, 490
multiple Tomcat instances on UNIX....116, 119
Oracle iPlanet Server....116
primary servers....45
sample clients....480
secondary servers....47
servers....108
services on Windows....114
Telephony server....185
TSQS server....185
Web Management servers....114
Web Services server....114, 117, 119, 491, 492
Website on UNIX....117, 119
Workflow server....189, 232
starting servers....107

status, email ... 367
stopping
ADU server ... 107
CIRS server on UNIX ... 116, 118
Client SDK server ... 117, 120, 477, 478
EDU server ... 107
ICM server on UNIX ... 115, 118
multiple Tomcat instances on UNIX ... 117, 119
Oracle iPlanet Server ... 116, 119
services on Windows ... 114
Web Services server ... 117, 120, 491, 492
Website on UNIX ... 117, 120
stored procedure library, qdb2sp ... 123
string table messages
deleting ... 512
translating ... 512
Suggested Email Responses ... 248
sys_agentsearch.update_agentstate_cache ... 397
sys_transfer.transfertovq ... 396
sys_transfer.update_vq_cache ... 396
system store, database schema ... 54, 58
system workflows ... 82

T

target encoding ... 505
task ceiling ... 382
task load ... 382
Telephony
ACDname parameter ... 173
configuring ... 172
configuring Workflow server ... 187
documents ... 26
prerequisites ... 173
RONA ... 172
routing hints ... 191
Workflow server ... 186
workflows ... 189
Telephony server
about ... 174
CM ... 175
creating ... 174
starting ... 185
temp tablespace name ... 139, 149
templates, email ... 353
test agents ... 378
testing

agent installation ... 404
agents ... 378
Avaya Agent Web Client ... 466
time zones, Web Scheduled Callback ... 258

timeout ... 135, 145
tips
agent accounts ... 376
Avaya Agent installation ... 399
Data server ... 124
Design & Administration Tools ... 34
server installation ... 32, 33
Web Scheduled Callback ... 257
Tomcat
autostart on UNIX ... 117, 120
Setup ... 522
SSL ... 492
tools, Citrix ... 440
Traditional Chinese
HTTP Connector server ... 514
Notification server ... 513
TransferFlowName ... 389
translating, string table messages ... 512
troubleshooting
uninstalling ... 496, 497, 498, 499
Trusted Sites ... 399, 445
TS flows ... 82
TS server
see Telephony server
TS.IncomingCall ... 189
TSQS server
CM ... 184
Communication Manager ... 184
creating ... 183
starting ... 185
TsQueueStatistics server
see TSQS server
tuning parameters, servers ... 85

U

UADStringFormat ... 389
UICountryOrRegion ... 511
UILanguage ... 510
UNC to UNIX mapping
about ... 454
configuring ... 456
examples ... 455
prerequisites ... 454
requirements ... 454
Unified Agent Directory
configuring agents ... 388
configuring Workflow server ... 395
uninstalling
agent desktop applications ... 499
Avaya IC ... 496

Avaya IC servers ... 497, 498
FTSE for AIX ... 498
FTSE for Solaris ... 497
FTSE for Windows ... 496

Windows ... 496
updates
automatic ... 406
language pack ... 406

point patch 406
service pack 406
updating
ADU server 85
Directory server 142
DUStore server 86
index on AIX 256
index on Solaris 253
index on Windows 249
version.html 407
Web browser tool for Citrix 435
Workflow server 94
upgrading 64

V

verifying
permissions for ECB 61
version.html 407
vesp.imp, copying 403
voice
prerequisites 173
Workflow server 186

W

WACD flows 82
WACD server
see WebACD server
WACD.QualifyChat 232
WACD.QualifyEmail 345
WAR file
deploying 462
Web application
Email Template Administration 333
Website 210, 219, 224
Web browser tool
CitrixClientURL 435
components 434
configuring 433
DontStartMultipleInstancesOfAgent 435
installing 434
multiple Citrix servers 436
updating HTML page 435
Web Client
see Avaya Agent Web Client
Web License Manager
changing password 168
installing license 165
JVM Options 522
Web Management
administration pages 226
configuring 194
configuring Workflow server 230
ICM server 237
optional configuration 194
refreshing IC Manager 286
RONA 194
routing hints 234
servers 206
starting servers 114
website 241
website account 79
Workflow server 229
workflows 232
Web Scheduled Callback
agent desktop applications 258
calendar 258
configuring 257
creating server 258
guidelines 258
requirements 257
time zones 258
Website 259
Web Services
configuring 490
deploying 484
documents 26
files 485
installing 485
prerequisites 484
secondary ORB server environment 485
SSL 492
starting server 491
stopping server 491
Web Services Bridge 485
Web Services Bridge
agent account 486
creating 487
domain 488
setting up 485
Web Services server
starting 114, 117, 119, 491, 492
stopping 117, 120, 492
Web tab, advanced properties 520
WebACD server 196, 210
changing service port 518
creating 196
Email Management 352
WebLM server 168
Website
account 79
administration 277
configuring 206, 241
customer 279
enabling CIRS servlet 285
JVM Options 522
Web application 210, 219, 224
Web Scheduled Callback 259
website account 79

websitecontext....285
Windows
Avaya Agent Web Client
starting....463
stopping....463
configuring full-text searches....248
installing Avaya Agent Web Client connector....37
installing Client SDK....37
installing Design & Administration Tools....37
installing Server SDK....63
installing servers....37
starting Client SDK server....114, 477
starting services....114
starting Web Services server....114, 491
stopping Client SDK server....477
stopping services....114
stopping Web Services server....491
updating full text index....249
Workflow server
agents....395
chat....229
configuring for Email Management....343
configuring for Telephony....187
configuring for Web Management....230
email....342
loading flows....190
restarting....348
starting....189, 232
updating....94
voice....186
workflows
documents....27
Email Management....348
incoming email....191
loading....190
qualify chat....234
qualify email....350
sample....82
system....82
Telephony....189
Web Management....232
WorkflowServerName....389
working directory
Avaya Agent Web Client....447
Client SDK....392
configuring....390, 392

X

XML encoding....505
X-Windows....31, 155