Avaya Interaction Center
Administration Guide

Release 7.3.x
Issue 5
February 2019

© 2012-2017 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:

https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

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

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

License type(s)

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

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third party components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including

open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at:

https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction . . . 22
- Purpose. . . . 22
- Intended audience . . . 22
- Document changes since last issue . . . 22
- Related resources . . . 23
  - Documentation. . . . 23
  - Training. . . . 23
  - Viewing Avaya Mentor videos . . . 24
- Support . . . 24

Chapter 2: Administration overview . . . 26
- Determining the structure of Avaya IC . . . 27
- Implementing Avaya IC structure. . . . 29
- Overview of Avaya IC Manager . . . 31
  - Customizing Avaya IC Manager . . . 33
  - Locking Avaya IC Manager . . . 35
  - Exiting Avaya IC Manager. . . . 35
  - Getting help . . . 35
  - Running multiple instances of Avaya IC Manager. . . . 36
- Avaya IC administration tasks . . . 36
  - Managing sites. . . . 37
  - Changing the administration password . . . 38
  - Backing up and restoring server configuration information . . . 38
  - Setting database connection information . . . 41
  - Setting Avaya IC Manager log levels . . . 42
  - Avaya IC Manager log file maintenance . . . 43
  - Setting environment information . . . 43
  - Monitoring alarms . . . 45
  - Resetting the system time zone on Avaya IC systems . . . 46
  - Tuning and maintaining the Avaya IC database . . . 46
  - Configuring clusters. . . . 47

Chapter 3: Domains . . . 52
- Setting up your domains . . . 53
- Creating your domains . . . 54
- Assigning servers to a domain . . . 55
- Creating failover domains. . . . 56
  - Preconfigured Failover Domains . . . 57
- Assigning agents to the domains . . . 61

Chapter 4: Managing servers 62
Server overview 64
Changing server information 67
General tab 68
Server tab 69
Configuration tab 70
Debug tab 70
Advanced tab 73
Creating a server. 74
Determining server start up or shutdown dependencies 75
Server startup dependencies 75
IC Shutdown Dependencies. 76
Starting or stopping a server 78
Updating server information 79
Copying or moving a server 79
Deleting servers 79
Synchronizing multiple Directory servers 80
Configuring Web Management servers 81
Understanding Web Management servers 83
WebACD server statistics 83
Working with WebACD tasks 84
Viewing ICM service status 86
Viewing historical chat logs. 87
Enabling the SSL security for the Directory server 87
Enabling the SSL security for the HTTPConnector server 88

Chapter 5: Email services 90
Email template administration 90
Managing templates and statuses 91
Email templates with attachments 93
Organizing the content 93
Creating templates. 93
Modifying a template 94
Refreshing email templates 95
Deleting email templates 95
Multi-language support for email templates 96
Creating folders and sub-folders 96
Modifying a folder 97
Creating statuses 98

Modifying a status . . . 99
Setting the Answered status to a message . . . 99
Applying an autoresponse template to a status . . . 100
Associating resolve statuses with email templates . . . 101
Associating the template with a status . . . 101
Template macros . . . 102
File attachments . . . 104
Sample message templates . . . 105
Avoiding an email auto response loop . . . 106
Formatting email text . . . 107
Changing the message format . . . 108
Formatting an HTML email message . . . 108
Formatting message text . . . 109
Aligning text . . . 109
Changing the font colors . . . 109
Creating a bulleted or numbered list . . . 110
Inserting an image . . . 110
Email accounts . . . 111
Adding an email account . . . 111
Testing an email account . . . 117
Configuring email account on Microsoft Exchange for the website to send emails . . . 119
Settings for Microsoft Exchange 2010 . . . 119
Settings for Microsoft Exchange 2013 . . . 121
Email filters . . . 123
Creating email filters in IC 7.3, 7.3.1, and 7.3.2 . . . 123
Creating email filters in IC Release 7.3.3 and later . . . 124
Email Filter tool for testing email filter regular expressions . . . 125
Retrieve exact matches in email From address search . . . 127
Deleting an email account . . . 127
Failure scenarios for incoming emails . . . 128
Email approval process . . . 129
Create a routing hint for email approval . . . 129
Create an approval workgroup . . . 130
Create an approval queue . . . 131
Create agents for the approval workgroup . . . 132
Configure the IC Email server to analyze outbound emails . . . 132

Chapter 6: Additional configuration options . . . 136
Creating new records . . . 137
Changing records . . . 138

Deleting records 138
Default properties 138
Chat table folder 139
Private Key PassPhrase table folder 144
Resource Manager table folder 145
Telephony table folder. 145
Voice Chat table folder 146
Website table folder 148
WorkFlow table folder 150
Configuring LDAP 152
Directory Server 152
Design and Admin 154
Adding secure email code in the custom website. 168

Chapter 7: Using Content Analyzer for automated email processing 170
Setting up Content Analyzer 171
Customizing the display of warning messages 172
Designing the topic trees 173
Creating topic trees 174
Working with topics 175
Working with samples. 176
Tagging samples and creating sample sets 177
Creating a list of samples 178
Associating topics and creating sample sets 180
Creating individual samples 181
Working with Knowledge Bases 182
Creating a Knowledge Base. 182
Training a Knowledge Base. 183
Interpreting training results. 184
Validating a Knowledge Base. 185
Interpreting validation results 187
Putting the validated Knowledge Base into production 189
Maintaining your Knowledge Bases 190
Updating topic trees 190
Synchronizing a Knowledge Base 192
Maintaining your samples and sample sets 193
Examining sample sets 193
Creating new sample sets from existing sets 193
Removing sample sets 195

Removing samples 195

Chapter 8: Avaya IC Report Wizard. 198
Using the Avaya IC Report Wizard 198
The Report Wizard interface 199
Displaying detailed contact information 200
Contact form 200
Customer form 202
Queue form. 202
Retrieving basic contact information. 202
Specifying what data the Report server collects 204
Core Tables 204
Reference Tables 205
The Mapping specification 206
Customizing the data model 207
Difference between the EDUID stored in Report Server and DUStore 208
Modifying creation rules and field expressions 208
Viewing and creating rules and expressions 210
Field expression functions 210

Chapter 9: Managing Agents 214
Prerequisites 214
Agent information 214
Using the Agent Manager 215
Creating a new agent 216
Entering basic agent information. 217
Configuring channels 223
Setting agent security information 226
Assigning agent properties 230
Defining agent skills. 231
Setting Business Advocate information 233
Setting miscellaneous agent information 234
Creating accounts for non-human agents 234
Adding a non-agent member to the Unified Agent Directory or Address Book 236
Searching for agent records 236
Sorting agent listings 237
Changing agent information 237
Changing multiple agent records. 238
Updating the database. 239

Deleting an agent 239

Chapter 10: Workgroups and tenants 240
Properties 241
Tenants 241
Creating a tenant. 242
Workgroups 242
Sample organization. 244
Grouping rules 245
Creating tenants and workgroups 245
Creating tenants 246
Creating workgroups 246
Assigning tenant and workgroup properties 248
Displaying inheritance information. 249
Modifying tenants and workgroups 250
Deleting tenants and workgroups 251

Chapter 11: Avaya IC Customer HTML Chat Client 252
About the Customer HTML Chat Client 252
Chat features supported by the Customer HTML Chat Client 253
Customization features of the Customer HTML Chat Client 254
Limitations of the Customer HTML Chat Client 255
Required software for the Customer HTML Chat Client. 255
Required Avaya IC servers and prerequisites 255
Supported Web browsers for Website customers. 256
Customizing tenant website properties 256
Modifying the tenant website properties. 257
Modifying the CSPortal chat window idle timeout. 258
Configuring the chat client deployment 259
Configuring Page Push from customers. 260
Modifying the Collaborative Form-filling properties for customers 260
Modifying the Collaborative Form-Filling properties for Workgroups and Agents . 261
Changing the HTML Chat Client properties 262
Customizing the logo 263
Changing the window position and size 264
Changing the frame sizes 265
Customizing the background colors 266
Customizing the text entry fields 266
Customizing the welcome message 266
Customizing the chat transcript 267

Customizing the timestamp on chat transcripts . . . 273
Customizing the tooltips . . . 274
Adding a help file . . . 275
Enabling the debug window . . . 276
Disabling the Enter event . . . 276
Emoticons . . . 277
Configuring Avaya IC Manager to enable emoticons . . . 278
Chat typing status . . . 278
Configuring blind chat transfer . . . 281
Example: Changing the images for a button . . . 282
Localization properties . . . 283
Chat Timestamp feature . . . 283
Importing the SC.xml file . . . 284
Enabling the TimeStamp feature . . . 284
Troubleshooting the Website Multi-Tenant Administration pages . . . 285
Troubleshooting the Customer HTML Chat Client . . . 286
Frame killer in pushed Web page unloads chat session . . . 286
Customer HTML Chat Client does not open in pop-up window . . . 287
Customer requests chat transcript after session closed . . . 287

Chapter 12: Advanced agent settings . . . 288
Setting up the home directory and working directory . . . 288
Directory properties for agent applications . . . 289
Purpose of the directory properties . . . 289
Recommended deployments for the home directory and working directory . . . 290
Configuring the home directory . . . 291
Configuring the working directory . . . 292
Configuring UNC to UNIX path mapping . . . 293
Using a shared directory for agent files . . . 295
Using a shared directory for agent user documents . . . 297
Creating shared resources for agents . . . 298
Customizing the Web Agent . . . 299
Web Agent interface . . . 299
Configuration files . . . 299
WebACD server configuration options . . . 301
Configuring RONA for the chat channel . . . 301
About contact acceptance RONA . . . 301
About agent confirmation . . . 302
Configuring agent confirmation for Avaya Agent desktop . . . 302

Configuring agent confirmation for Avaya Agent Web Client 302
About the default timeout 303
Configuring the default timeout for Avaya Agent desktop 303
Configuring the default timeout for Avaya Agent Web Client 303
Changing the default RONA behavior for chat contacts 304
Configuring RONA for the email channel 304
Types of RONA for the email channel 305
Configuring contact acceptance RONA for the Avaya Agent desktop. 305
Configuring contact acceptance RONA for Avaya Agent Web Client 306
Modifying the time limit for email activation RONA in the Avaya Agent desktop . . 306
Changing the default RONA behavior for email contacts. 307
Creating wrap up, AuxWork, and Logout codes. 308
General code administration tasks 309
Wrap up codes 310
AuxWork and Logout codes 313
Audio and visual notifications for the chat channel. 315
Configuring audio and visual notifications for the chat channel. 316
Customizing sound alerts 317
Customizing the window for the popped out chat tab 318

Chapter 13: Document search facilities 320
Setting up the Web Self-Service feature 320
Administering the FAQ database 321
Managing the FAQ database 321
Submitting new documents 322
Reviewing agent-proposed documents 323
Editing and deleting existing documents 324
Searching for specific documents 324

Chapter 14: Tenant websites 326
Enabling website language options 327
Adding a new language 327
Enabling a language for a tenant 328
Deleting a language 328
Internationalized language options. 328
Customizing tenant websites 329
Customizing tenant website properties 330
Customizing tenant source code 331
Specifying the URL for the tenant’s index page 332
Customizing account information 332

Customizing standard properties . . . 333
Adding new user properties . . . 333
Working with customer accounts . . . 334
Creating customer accounts . . . 335
Modifying customer accounts . . . 335
Enabling and disabling customer accounts . . . 336
Understanding the default account management process . . . 337
Setting up the WebSchedule Callback feature . . . 339
Configuring WebSchedule Callback properties . . . 339
Setting up Shared Browsing . . . 340
Collaborative Form-filling . . . 340
Using the DataWake feature . . . 341
Filters and regular expressions . . . 342
Ripple regular expressions . . . 342
Setting up filters on multiple web servers . . . 342
Syntax for regular and ripple expressions . . . 344
Setting up DataWake filters . . . 346
Adding regular and ripple regular expressions . . . 347
Ordering expressions . . . 348
Modifying or deleting expressions . . . 349
Viewing DataWake records . . . 350
Full DataWake history . . . 350
Viewing your own DataWake record . . . 351
Using the Email History feature . . . 351
Enabling the Email History feature . . . 351
Accessing the Email History feature . . . 353
Viewing the Email History report . . . 354
Exporting the Email History report . . . 355
Copying the Email History report . . . 356
Searching an email message in the report . . . 356
Displaying the email message text . . . 356
Showing the number of records in the report . . . 356
Sorting the report list . . . 357
Using the Chat History feature . . . 357
Enabling the Chat History feature . . . 358
Accessing the Chat History feature . . . 359
Viewing the Chat History report . . . 360
Exporting the Chat History report . . . 361
Copying the Email History report . . . 362
Searching a chat communication in the report . . . 362

Displaying the chat communication details 362
Showing the number of records in the report 363
Sorting the report list 363

Chapter 15: Properties 364
Property inheritance 365
Cumulative property inheritance 365
Non-cumulative property inheritance 366
Sample inheritance scheme 367
Setting up properties and property sections 369
Creating property sections 370
Creating properties 370
Changing properties 372
Changing property sections 372
Changing property names and datatypes 372
Changing property settings 373
Changing property values 373
Deleting properties 374
Deleting property sections 374
Deleting properties 374
Deleting property values 374

Chapter 16: Devices and queues 376
Creating devices 378
Specifying general device information 379
Assigning devices to workgroups 381
Specifying voice configuration options 382
Specifying Business Advocate parking device configuration options 383
Creating virtual queues 384
Changing device information 385
Viewing the contacts handled by each device 385
Deleting devices 386

Chapter 17: Tables 388
Creating tables 388
Deleting tables 389
Entering and changing table information 390
Table import and export 391
Exporting a table 391
Reserved table names 392

Appendix A: Database tuning and maintenance 394
Consulting a qualified database administrator 394
Database tuning guidelines 395
Database table growth rates 395
Database queries 397
Transaction logs 397
Database maintenance 398
Scheduling maintenance procedures 398
Using database tools to check performance 398
Creating a backup strategy 399
Backup responsibilities 399
Types of backups 400
Minimum frequency of backups 400
Recommended backup strategies 400
Creating a purging strategy 401
Considerations for a purging strategy 401
Recommended criteria for purging strategy 402
Running optimization procedures 402
Relationships between database tables 403
Historical contact data 404
Email contact data 404
Chat contact data 405
Related documentation 405

Appendix B: Database Purge 406
Database purge of IC Repository and CallCenterQ database tables for MSSQL 2008, 2010, and 2014 406
Guidelines for purging of emails from IC Repository and CallCenterQ database tables 406
Overview of the purging process 407
Purging of data from the IC Repository and the CallCenterQ database tables - High level steps 408
Purging of data from the IC Repository database tables 409
Purging of data from the CallCenterQ database tables 410
Database purge of IC Repository and CallCenterQ database tables for Oracle 10g and Oracle 11.x g 411
Guidelines for Purging of emails from IC Repository and CallCenterQ database tables 411
Overview of the purging process 411
Purging of data from the IC Repository and the CallCenterQ database tables - High level steps 413
Purging of data from the IC Repository database tables 414
Purging of data from the CallCenterQ database tables 415

Appendix C: Server configuration reference 418
Before configuring servers 419
ADU (Agent Data Unit) server 420
General tab 421
ADU tab 421
Persistence tab 426
Configuration tab 427
Debug tab 428
Advanced tab 428
Alarm server 428
General tab 429
Alarm tab 429
Debug tab 431
Attribute server 432
General tab 432
Attribute tab 433
Debug tab 434
Blender server 434
General tab 435
Blender tab 435
Watch tab 436
Configuration tab 438
Debug tab 438
CAAdmin (Content Analyzer Administration) server 438
General tab 439
CAAdmin tab 440
Debug tab 440
CA (Content Analyzer) server 440
General tab 441
CAServer tab 441
Debug tab 443
ComHub server 443
General tab 444
ComHub tab 444
Debug tab 445
Data server 445
General tab 446
Debug tab 446
DataServer tab 446

DataServer tab for IBM DB2 . . . 447
DataServer tab for MSSQL Server . . . 448
DataServer tab for Oracle . . . 450
DataServer tab for ODBC . . . 452
Directory server . . . 453
General tab . . . 453
Directory tab . . . 454
Configuration tab . . . 456
Advocate tab . . . 457
Debug tab . . . 457
DUStore server . . . 458
General tab . . . 458
DUStore tab . . . 459
Debug tab . . . 459
EAI server . . . 460
EAI Email server . . . 460
EAI Workflow server . . . 460
EDU (Electronic Data Unit) server . . . 460
General tab . . . 461
EDU tab . . . 462
Persistence tab . . . 467
Debug tab . . . 468
Event Collector server . . . 469
General tab . . . 469
EventCollector tab . . . 470
Debug tab . . . 471
Event Collector Bridge server . . . 472
General tab . . . 472
Event Collector Bridge tab . . . 473
Debug tab . . . 473
HTTP Connector server . . . 473
General tab . . . 474
Configuration tab . . . 474
HTTPConnector tab . . . 475
Debug tab . . . 477
HTTPVOX server . . . 477
General tab . . . 478
HttpVOX tab . . . 479
Configuration tab . . . 481

Debug tab 481
Advanced tab 481
Email server 482
General tab 482
ICEmail tab 483
Configuration tab 485
Debug tab 485
Log Collector server 485
General tab 488
LogCollector tab 488
Debug tab 488
Java Application Bridge server 488
General tab 489
JavaAppBridge tab 490
Debug tab 492
License server 493
General tab 493
License Server tab 493
Debug tab 494
Advanced tab 495
Notification server 496
General tab 496
Notification tab 497
Debug tab 499
Polling 499
ORB server 500
General tab 501
ORB tab 501
Debug tab 501
Paging server 502
General tab 502
Paging tab 503
Debug tab 503
Poller server 504
General tab 504
Poller tab 504
Configuration tab 509
Debug tab 509
Report server 510

General tab 510
Report tab 511
Configuration tab 512
Debug tab 513
Resource Manager server 513
General tab 513
Resource Manager tab 514
Configuration tab 514
Debug tab 515
SiebelAED server 515
SiebelAICD server 515
SiebelASIS server 515
TS (Telephony) servers 515
General tab 516
TS tab 516
TS tab for Avaya Communication Manager 517
Configuration tab 522
Hetero-switch tab 522
Advocate tab 525
Debug tab 525
Telephony Queue Statistic servers 526
General tab 526
Debug tab 526
TSQS tab 527
TSQS tab for Avaya Communication Manager 527
TSA (Telephony Services Adaptor) server 528
General tab 528
TSA tab 530
Debug tab 531
VOX server 531
General tab 532
VOX tab 532
VRU tab 538
Configuration tab 539
Debug tab 539
WAA (Web Advocate Adaptor) server 540
General tab 540
WAA tab 541
Debug tab 542

WebACD server 542
General tab 543
WACD tab 543
Advocate tab 547
Configuration tab 547
Debug tab 550
Web Scheduled Callback server 550
General tab 551
WSCallback tab 551
Debug tab 553
WebServices server 553
General tab 554
WebServices tab 554
Debug tab 556
Workflow server 556
General tab 557
WorkFlow tab 558
Channels tab 560
Debug tab 563
Recommended server parameter settings 564
Configuration Tool settings 564

Appendix D: Typing special characters 566

Appendix E: Property descriptions 570
Admin property descriptions 570
Admin/Agent properties 570
Admin/Agent/Channel properties 572
Admin/General properties 573
Admin/Server properties 573
Agent property descriptions 574
Agent properties 575
Agent/Desktop properties 577
Agent/Desktop/AddressBook properties 586
Agent/Desktop/Chat properties 587
Agent/Desktop/Chat/Application properties 588
Agent/Desktop/ContactSuspension properties 590
Agent/Desktop/CustomerContacts properties 591
Agent/Desktop/Directory properties 592
Agent/Desktop/Directory/SkillProficiency properties 595

Agent/Desktop/Directory/Voice properties . . . 596
Agent/Desktop/Email properties . . . 597
Agent/Desktop/Email/AlertInfo/REQ properties . . . 599
Agent/Desktop/Email/AlertInfo/SME properties . . . 600
Agent/Desktop/Email/Application properties . . . 601
Agent/Desktop/Prompter properties . . . 605
Agent/Desktop/QuickFind properties . . . 606
Agent/Desktop/Resources properties . . . 606
Agent/Desktop/ScreenPop properties . . . 607
Agent/Security properties . . . 609
Agent/Desktop/Softphone properties . . . 611
Agent/Desktop/Spelling properties . . . 612
Agent/Desktop/StatusBar properties . . . 615
Agent/Desktop/Voice properties . . . 617
Agent/Desktop/WAC properties . . . 622
Agent/Desktop/WebClient properties . . . 624
Agent/Desktop/WebClient/Connection properties . . . 627
Agent/Desktop/WebClient/Preferences properties . . . 628
Agent/Desktop/WebClient/Preferences/PreferredWorkload properties . . . 628
Agent/Desktop/WrapUp properties . . . 629
Agent/Desktop/WrapUpDialog properties . . . 630
Contact/AgentDesktop property descriptions . . . 631
Email property descriptions . . . 632
Email/Agent properties . . . 632
Email/Runtime properties . . . 632
QUI property descriptions . . . 633
QUI/General properties . . . 633
System/Configuration property descriptions . . . 644
Voice/Configuration property descriptions . . . 646

Index . . . 650

Chapter 1: Introduction

Purpose

The purpose of this guide is to provide detailed information about Avaya Interaction Center (Avaya IC). This guide describes domain and server administration using Avaya IC Manager.

Intended audience

This guide is for the customers using Avaya Interaction Center. You must use this guide for adding, modifying, deleting, and monitoring Avaya IC servers on your Avaya IC system.

The audience for this guide includes:

- Application consultants
- Integration consultants
- Avaya BusinessPartners
- Customers

Document changes since last issue

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

- Recommended Server parameter settings
- ICM record properties
- WebACD task priority
- Recommended server parameter settings
- Chat Timestamp feature

Related resources

Documentation

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

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: Administration overview

Avaya Interaction Center (Avaya IC) is a complete multi-media system that helps the contact center to route and manage transactions across multiple channels including voice, email, chat, and web-based e-commerce. Avaya IC routes customers to the best resource at the contact center and records the details of their transactions.

To support all these channels, Avaya IC includes a set of media connectors that link to email systems, e-commerce software, Interactive Voice Response (IVR) units, and Automatic Call Distribution (ACD) telephone switches. These connectors link the different media systems to the Avaya IC Engine to provide a single point of control across all of the channels.

The system administrator must understand the following terms as they are used on the Avaya IC system:

Term	Definition
Agent	The individual who receives and handles contacts at the contact center. Agents are sometimes called Customer Support Representatives.
Domain	A set of servers that work together to service requests. When a contact enters Avaya IC, several servers must interact to handle the contact. A domain specifies which servers work together. Agents are assigned to domains to determine the servers that will service their requests.
Properties	Customizable settings assigned to the Avaya IC environment, tenants, workgroups, or agents. After assignment, the properties are stored in the Avaya IC database. An Avaya IC system accesses the database to retrieve the property settings. Properties can be used to define the colors displayed on a workstation, the shape of the buttons, or the behavior of the agent's applications.
Device	A channel specific queue, a virtual queue, or a parking area. When contacts are placed in a queue, they are routed to the next available agent. When contacts are placed in a parking device, they are held indefinitely until an agent becomes available.
Server	The software that performs functions in Avaya IC. For example, the Telephony server is responsible for receiving messages from the telephone switch and passing the information to other servers, and the Directory server maintains an accurate list of agents and servers on the system.
Site	The physical location of agents, servers, or queues. Avaya IC uses the site information when it makes routing decisions, linking, and call flow optimization.

Term	Definition
Tenant	A set of workgroups organized around a particular business function. A tenant is used to define the security and administrative boundaries around data, queues, and content resources. An agent or queue can belong to multiple tenants, but a workgroup can only belong to a single tenant. Tenants are usually organizations within your company, but if you outsource webhosting services, they can be the individual companies that use your services.
Workgroup	A set of agents or queues grouped together so that the administrator can view information about the agents in the context of the group. For example, agents can be grouped based on the type of contacts they handle or the agents can be grouped by their department name.
Cluster	A set of two identical servers grouped together to achieve the redundancy. In a set, one server acts as a primary server and the other server as a secondary server. You can create separate groups for two Avaya IC Email or two WebACD, or two Poller servers.

This section contains the following topics:

- Determining the structure of Avaya IC on page 27
- Implementing Avaya IC structure on page 29
- Overview of Avaya IC Manager on page 31
- Avaya IC administration tasks on page 36
- Tuning and maintaining the Avaya IC database on page 46

Determining the structure of Avaya IC

Before you begin working with the Avaya IC software, you must plan the implementation of the system and how it must behave when telephone calls, emails, faxes, or chat requests come into your contact center. Each element of Avaya IC builds on the ones before it.

Tip:
For example, an agent must be assigned to only one domain. Therefore, you must define your domains before you define your agents. Otherwise, you will have to assign all of your agents to the default domain and move them later. You must decide the following:

- The number of sites in your Avaya IC environment. For details, see Managing sites on page 37.
- The number of domains you need to create. For details, see Chapter 3: Domains on page 52.

- Which servers should be created within each domain. For details, see Chapter 4: Managing servers on page 62.
- Which agents should be assigned to each domain.
- What devices need to be created.
- What sets of agents and devices should be organized into workgroups.
- What sets of workgroups should be organized into tenants.
- The properties that should be associated with all agents, workgroups, and tenants.
- The inheritance rules governing all properties.
- Whether you want to set up a Web Self-Service database so that employees or customers can search through a database of solutions on the web.
- Whether you want to create a collection of documents that agents can search for problem solutions.

For details about agents, devices, workgroups, tenants, properties, Web Self-Service, and document collections, see *IC Administration Guide*.

You need to decide:

- The number of sites in your Avaya IC environment (for details, see Managing sites on page 37)
- The number of domains in your system
- Which servers should be created within each domain
- What agents need to be created (for more information, see Chapter 9: Managing Agents on page 214)
- What devices need to be created (for details, see Chapter 16: Devices and queues on page 376)
- What sets of agents and queues should be organized into workgroups (for details, see Workgroups on page 242)
- What sets of workgroups should be organized into tenants (for details, see Tenants on page 241)
- What properties should be associated with all agents, workgroups, and tenants (for details, see Chapter 15: Properties on page 364)
- Whether you want to set up a Web Self-Service database so that employees or customers can search through a database of solutions on the web (for more information, see Setting up the Web Self-Service feature on page 320)
- Whether you want to import legacy data from other databases into the Avaya IC system.

Tip:
For details about servers, domains, and legacy data, see *IC Administration Guide*.

You need to decide the following:

- The number of sites in your Avaya IC environment (for details, see Managing sites on page 37)
- The number of domains you need to create (for details, see Chapter 3: Domains on page 52)

- Which servers should be created within each domain (for details, see Chapter 4: Managing servers on page 62)
- What agents need to be created (for details, see Chapter 9: Managing Agents on page 214)
- What devices need to be created (for details, see Chapter 16: Devices and queues on page 376)
- What sets of agents and queues should be organized into workgroups (for details, see Workgroups on page 242)
- What sets of workgroups should be organized into tenants (for details, see Tenants on page 241)
- What properties should be associated with all agents, workgroups, and tenants (for details, see Chapter 15: Properties on page 364)
- Whether you want to set up a Web Self-Service database so that employees or customers can search through a database of solutions on the web (for details, see Setting up the Web Self-Service feature on page 320)

Implementing Avaya IC structure

After you decide the structure of your Avaya IC environment, you can implement that structure using Avaya IC Manager. For details about the Avaya IC Manager interface, see Overview of Avaya IC Manager on page 31.

Note:
The Contact Engine servers, specifically the ORB server, the Alarm server, and the Directory server must be installed, configured, and functional before you can run Avaya IC Manager. For detailed instructions, see IC Installation and Configuration.

To begin using Avaya IC Manager:

1. From the Windows **Start** menu, click **All Programs** > **Avaya Interaction Center 7.3.x** > **Avaya IC Manager**.

   The system displays the **Avaya IC Manager Login** dialog box.

   Note:
   To use Avaya IC Manager, your Windows logon ID must have administrator privileges on a computer running Avaya IC Manager. If your ID does not have administrator privileges, see your System Administrator.

2. If you already have a user account with the minimum required security privileges, enter your login ID and password, and then click **OK**.

   For details, see Setting agent security information on page 226.

   If user accounts have not yet been set up, use the out-of-the-box administrative account (login ID: **Admin**, Password: **admin**). The first time you use this account to login in to Avaya IC Manager after your database has been configured, you must change the default password for security reasons. For details, see Changing the administration password on page 38.

If the login is successful, the main Avaya IC Manager window appears. If the login is unsuccessful, check your user name and password. If you have entered correct user name and password, ensure that ORB, Alarm, and Directory servers are running.

You can implement the required structure by:

1. Instantiating and configuring the Avaya IC servers, starting with the Data server. For details, see Chapter 4: Managing servers on page 62.
2. Instantiating and configuring the Avaya IC servers, starting with the Data server. For detailed instructions, see *IC Administration Guide*.
3. Instantiating and configuring the Avaya IC servers, starting with the Data server. For detailed instructions, see Chapter 4: Managing servers on page 62.

   Note:
   Before you configure agent, tenant, or workgroup administration, the database must be created and seeded as described in the *IC Installation and Configuration* guide.

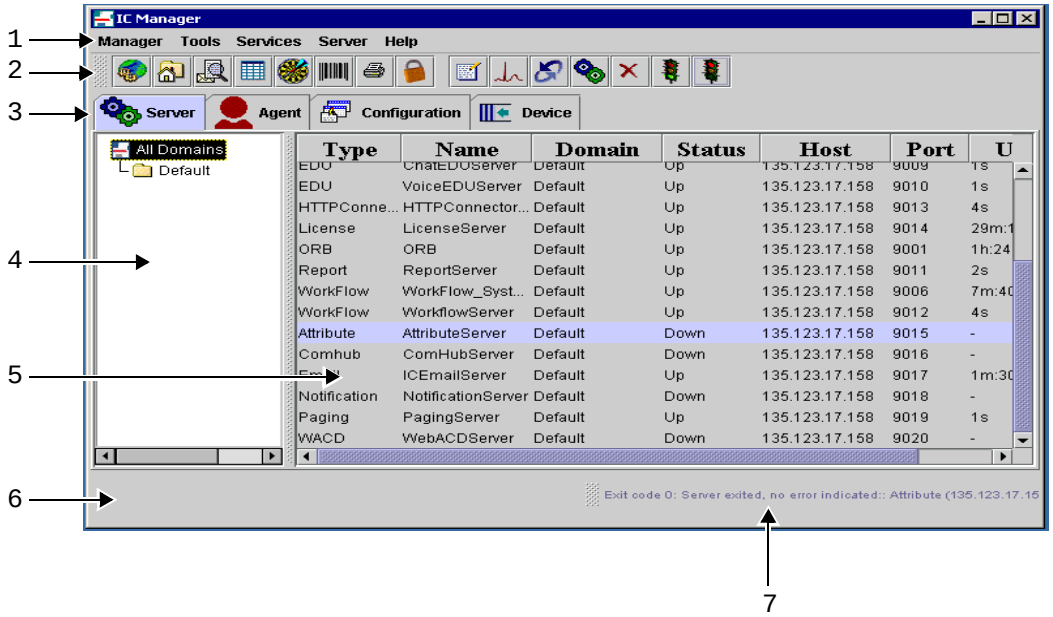
4. Configuring Email Management, if applicable to your contact center, as described in Chapter 5: Email services on page 90.
5. Configuring Email Management, if applicable to your contact center, as described in *IC Administration Guide*.
6. Configuring Email Management, if applicable to your contact center, as described in Chapter 5: Email services on page 90.
7. Creating domains for the Avaya IC servers as described in Chapter 3: Domains on page 52.
8. Setting up the agent environment by creating:
   - agents (for details, see Chapter 9: Managing Agents on page 214)
   - skills (for details, see Agent-skill associations on page 232)
   - tenants (for details, see Tenants on page 241)
   - workgroups (for details, see Workgroups on page 242)
   - devices (for details, see Chapter 16: Devices and queues on page 376)
   - properties (for details, see Chapter 15: Properties on page 364)

Overview of Avaya IC Manager

Avaya IC Manager is an administration and system management tool that helps you manage, configure, and monitor the components of Avaya Interaction Center (Avaya IC). With Avaya IC Manager, you can add, delete, and modify information for agents, servers, and devices. You can also configure the channels that are used by the agents to handle contacts. Avaya IC Manager lets you start and stop Avaya IC servers, and monitor the activities of servers, agents, and devices on Avaya IC.

The main Avaya IC Manager window displays information about the servers, agents, codes, configurations, and devices in Avaya IC. The amount of information Avaya IC Manager displays is based on your security privilege. Users with fewer privileges can only see a subset of options.

The default user account, Admin, has full access to all options on all screens. The information presented in this manual assumes that you have access to all options.



1. Menu Bar
2. Toolbar
3. Tabs
4. Left Pane
5. Right Pane
6. Status Bar
7. Alarm Summary

The Avaya IC Manager window consists of:

Menu bar: Contains menus that list the Avaya IC Manager options. The list of available menus changes based on the tab that you click.

Toolbar: Contains buttons for frequently used menu options. The toolbar displays the buttons based on the pane that you select.

Tabs: Lets you display the manager screens for Servers, Agents, Codes, Configuration, or Devices. You can also create user-defined tabs as described in Customizing Avaya IC Manager on page 33. Click the appropriate tab to display the required manager dialog.

Left and Right panes: Displays information for the selected manager. The left pane contains a tree structure that shows the elements within the selected manager. In the previous example, you can view the **Server** tab, which shows a tree view of all the domains defined in Avaya IC in the left pane.

The right pane displays details about the element that you select in the left pane. In the previous example, you can see that the **All Domains** element is selected in the left pane. So, the right pane displays the information about the servers in all of the domains. If you select a single domain, the right pane displays the servers in the selected domain.

Status bar: Notifies you of various activities:

- The current state of Avaya IC Manager, such as Working or Ready.
- An alarm summary that informs you of messages from Avaya IC. An alarm is a message that alerts you to an unexpected situation, such as a server becoming unavailable. Whenever an alarm is raised in Avaya IC, the graphic on this button changes to alert you of the situation. The Status Base also displays the description of the alarm message.

  Tip:
  You can display the **Alarm Monitor** dialog either by clicking the **Alarm Summary** button on the toolbar or by accessing **Alarm Monitor** from the **Tools** menu. For more information, see Monitoring alarms on page 45.

- Whenever there is network communication, for example, when Avaya IC Manager communicates with Avaya IC Engine server, a network icon is displayed next to the alarm monitor.

Sorting and resizing columns

You can change the way Avaya IC Manager displays the information on a tab by sorting or resizing a column. You can:

- Sort a column in ascending order by clicking on the column header
- Sort a column in descending order by holding Shift and clicking on the column header
- Resize of the columns by dragging the column heading borders.

Option selection methods

There are several ways to perform a task in Avaya IC Manager. For example, to edit a server definition, you can right-click the server and select **Edit**, click **Edit** on the toolbar, or double-click the server name. Where multiple options are available, this manual describes the most convenient method to perform a task.

Selecting multiple items

While viewing a list of items, such as a list of agents in the Agent Manager, you can select multiple items in the list in the following ways:

- Shift + click. Select an item and then hold down the **Shift** key while clicking on a second item. This selects all of the items between the first and second item that are selected.
- Control + click. Select an item and then hold down the **Ctrl** key while clicking on additional items. This lets you select non-contiguous items.

Tip:
If you select a large number of agents in the Multi Agent Edit mode, it can take Avaya IC Manager several minutes to process record change requests. During this time, Avaya IC Manager may not respond to any other requests.

To improve the overall performance, you must process agents in smaller groups.

Note:
When you open multiple agents in the Multi Agent Edit mode, you can apply the changes simultaneously to all those agents that you opened in the Multi Agent Edit mode.

This section contains the following topics:

- Customizing Avaya IC Manager on page 33
- Locking Avaya IC Manager on page 35
- Exiting Avaya IC Manager on page 35
- Getting help on page 35
- Running multiple instances of Avaya IC Manager on page 36
- Managing sites on page 37

Customizing Avaya IC Manager

Using the Customization option, you can add toolbar buttons to Avaya IC Manager that help you launch and manage Java components, Java frames, or native O/S executable files. When you add a Java component, you can also add a new tab to Avaya IC Manager that helps you manage the component directly.

Note:

Avaya IC Manager maintains customizations on a per-user name, per-computer basis. If you log in with the user name Admin and customize Avaya IC Manager, then a person logging in with the user name Supervisor cannot see those customizations. Therefore, if you want a particular customization to be available to several different users, you must log into Avaya IC Manager and perform the customization steps for each user name separately.

Additionally, if you want the user name Admin to have the same customizations on several different systems, you need to log in to each system and perform the customizations manually.

To customize the Avaya IC Manager window:

1. In Avaya IC Manager, from the main menu, select **Tools** > **Customize**.

   The system displays the **Customize** dialog box with a list of applications that you already added.

2. Click **Create new external tool**.

   Hold the mouse pointer on a button to display the tooltip.

3. From the drop-down list, select the type of application that you want to add.

   You can select Java Component, Java Frame, or an Executable.

   Note:

   In Avaya IC Manager, you can create new tab for a Java Component by selecting the **Add to tab panel** check box. Not all Java components can be added to this tab.

4. In the **Name** field, enter the name.

   The system displays the name on the button or the tab.

5. For a Java Component or a Java Frame, enter the class name in the **Class** field. The class name is applicable if you are adding a Java Component or Java Frame. The class must exist in your class path.

6. For an Executable, enter the path of an executable file in the **Executable** field and enter the arguments that are required for an executable in the **Arguments** fields.

7. At this point, you can:

   - Add the new component and return to the main Avaya IC Manager window by selecting **Ok**.
   - Add the new component but keep the **Customize** dialog open and available by clicking **Set**.
   - Discard your changes and return to Avaya IC Manager without adding the component by clicking **Cancel**.

8. In the main Avaya IC Manager window, select **Manager** > **Save** to commit the changes to Avaya IC Manager.

Locking Avaya IC Manager

You can prevent an unauthorized access to the Avaya IC Manager whenever the system is left running and unattended.

Click the **Lock** button on the toolbar to lock the Avaya IC Manager system. After the Avaya IC Manager system is locked, you can unlock it by entering the correct admin password.

You can also lock the Avaya IC Manager system by selecting **Manager** > **Lock**.

Exiting Avaya IC Manager

To end the Avaya IC Manager session:

1. In Avaya IC Manager, from the main menu, select **Manager** > **Exit**.
2. Click **Yes**.

Or

1. In Avaya IC Manager, click on **X** button at the top right corner of the window.
2. Click **Yes**.

Getting help

You can access online help either through the **Help** menu or through the **Help** toolbar button. The Avaya IC Manager online help is displayed in a Web browser that is default to your system.

The Help menu contains:

- The **Help Topics** option, which displays the administration information about Avaya IC Manager. You can access the complete Avaya IC Manager help through this option.
- Help entry for the currently selected tab in Avaya IC Manager.

  Note:
  This entry is optional and it appears for the tab for which the help is available.
- The **About Avaya IC Manager** option, which displays the name and version of the Avaya IC Manager.
- The **Alarm Monitor Help** option, which displays information about the IC server alarms. This option is available in the Help menu of the **Alarm Monitor** window. In the Avaya IC Manager, you can access **Alarm Monitor** by selecting **Tools** > **Alarm Monitor**.

The **Help** button displays the online help for the current tab.

Running multiple instances of Avaya IC Manager

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

CAUTION:
Simultaneous administration of servers, domains, and directory server tables in more than one Avaya IC Manager might cause corruption of configuration files and loss of configuration data. Even if different records are updated, data corruption might occur.

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

- Use only one instance of Avaya IC Manager at a time to administer servers.
- Determine which Avaya 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 Avaya IC Manager with the same login ID and password.

To run multiple instances of Avaya IC Manager, you must install the IC Manager program separately on each administrator system. There is no mechanism to perform multiple installations at one time. For installation information, see *IC Installation and Configuration Guide.*

When you run multiple instances of IC Manager, the IC Manager instances do not notify the changes to the IC Manager on the administrator system. Therefore, in IC Manager, you must click **Manager** > **Refresh** to display the changes.

Avaya IC administration tasks

The following tasks affect the performance of Avaya IC:

- Managing sites on page 37
- Changing the administration password on page 38
- Backing up and restoring server configuration information on page 38
- Setting database connection information on page 41
- Setting Avaya IC Manager log levels on page 42
- Avaya IC Manager log file maintenance on page 43
- Setting environment information on page 43
- Monitoring alarms on page 45

- Resetting the system time zone on Avaya IC systems on page 46
- Tuning and maintaining the Avaya IC database on page 46
- Configuring clusters on page 47

Note:
If you want to save your configuration settings, you must select **Manager** > **Save**. If you exit Avaya IC Manager without saving the updated settings, Avaya IC Manager restores the earlier settings.

Managing sites

A site is a physical location that agents or servers can occupy in your Avaya IC environment. You must set up a site for each physical location in your company so that Avaya IC can use the information when making routing decisions.

Creating Site

To create a site:

1. In Avaya IC Manager, from the main menu, select **Tools** > **Site**.
2. In the **Site Editor** windows, click **New**.
3. Enter the name and description of the new site.
4. Click **Ok**.

   The system adds the new site in the site list.

Editing Site

To edit a site:

1. In Avaya IC Manager, from the main menu, select **Tools** > **Site**.
2. In the **Site Editor** windows, select a site from the list and click **Edit**.
3. Edit the name and description of the selected site.
4. Click **Ok**.

   The system updates the selected site in the site list.

Deleting Site

To delete a site:

1. In Avaya IC Manager, from the main menu, select **Tools** > **Site**.

2. In the **Site Editor** window, select a site from the list and click **Delete**.

   Ensure that you are deleting the correct site.

3. Click **Ok**.

   The system deletes the selected site from the site list.

Exit or Close Site

To exit or close a site:

1. In the Site Editor window, click OK or **X** button at the top right corner of the window.
2. Click **Yes**.

Changing the administration password

To ensure the security of the system, you need to change the default password for the Admin account. You have to change the password the first time you log in to Avaya IC Manager after your database is configured. The default Admin account will be prompted the first time you log in.

To change the Avaya IC Manager password:

1. In the Avaya IC Manager, click the **Agent** tab.
2. In the left pane, select **IC** > **Administrators**.
3. In the right pane, double-click the Login Id **Admin**.

   The **Admin@User1** window opens. **User1** is the domain name for the Admin user.

4. Click the **Security** tab.
5. Enter the new password in the **Password** and the **Confirm** fields.

   Note:
   You cannot keep the **Password** field blank.

   For details about Agent/Security password properties, see *IC Administration Guide*.

6. Click **Ok**.

   The new password takes effect the next time you log in to the Avaya IC Manager.

Backing up and restoring server configuration information

Because the Directory server provides access to all data, it keeps track of all server configuration settings entered in Avaya IC Manager. The directory server writes the server information to a repository file called `IC_INSTALL_DIR\etc\ds.ffd` on its local computer.

Create a backup copy of the Directory server's repository file after configuring the servers, and continue to do backups on a routine basis.

Tip:
These backup procedures only save server information, so it is recommended that you also backup the database. Consult with your database administrator to perform backup procedures on the database.

Backing up the configuration file of the Directory server

To back up the configuration file of the Directory server

1. In the Avaya IC Manager window, click the **Server** tab.
2. In the left pane, select the **All Domains** node.
3. In the right pane, double-click the parent **Directory** server (marked with an asterisk [*]).

   The **Directory@Default** window opens.
4. Click the **Directory** tab.
5. In the **Backup** field, enter the backup filename.

   Avaya IC Manager automatically adds an FFD extension to the specified filename.

   Note:
   The name `ds.ffd` is a reserved filename in the Avaya IC system. Therefore, you must enter a name other than `ds`.
6. Click **Start**.
7. Click **OK**.

   Avaya IC Manager creates the backup file on a computer running the parent Directory server. The default directory for the backup file is `IC_INSTALL_DIR\etc`.

Restoring the Directory server

To restore the Directory server from a previously created backup directory file

1. In the Avaya IC Manager window, click the **Server** tab.
2. In the left pane, select the **All Domains** node.
3. In the right pane, double-click the parent **Directory** server (marked with an asterisk [*]).
4. Click the **Directory** tab.
5. Enter the previously created backup filename in the **Restore** field without the FFD extension. The file must be in the home directory of the Directory server (default: `IC_INSTALL_DIR\etc`).

   Note:
   All configuration changes since your last back up will be lost.
6. Click **Start**.
7. Click **Ok**.

Setting database connection information

Database connections define the properties needed to access a database through an Avaya Data server. Each database connection represents one data source where the tables used by an application are located. You use the data source connection name when you define a table to let Database Designer and the application know where the table is located.

A connection set links the data sources with the physical database connections. Each connection set contains one or more of the data sources used in the application. If you need to access tables from more than one data source in your application, such as the application database and IC Repository, include a connection for each data source in your connection set.

In Avaya IC Manager, the IC Data Source Connections dialog box displays the connection and connection set information for all of the databases defined in your application ADL file through Database Designer.

To display database connection information, select **Tools** > **IC Data Sources**. Avaya IC Manager displays the **IC Data Sources** dialog box.

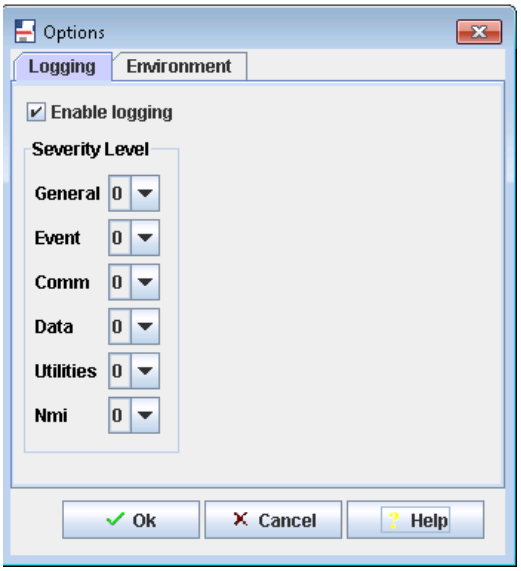
Note:
If the administrator changes the database connection information in Database Designer while you are running Avaya IC Manager, those changes will not be reflected in Avaya IC Manager automatically. To ensure you are viewing the most recent database connection information, select **Manager** > **Refresh**.

The right pane presents a tree view listing all of the data sources and their associated connections and connection sets. Select any element to view its details in the left pane.

For details about creating connections and connection sets, see the *IC Database Designer Application Reference*.

Setting Avaya IC Manager log levels

You can set the logging level according to which Avaya IC Manager writes to its log files. The higher the level you set, more detail information is stored in the log file.



CAUTION:
Increasing the logging of activity on Avaya IC may degrade the system performance. You should use minimal logging unless you encounter problems with Avaya IC.

To set the logging level:

1. In Avaya IC Manager, from the main menu, select **Manager** > **Options**.
2. Click the **Logging** tab.
3. Select the **Enable logging** check box.
4. From the **Logging type** drop-down list, select the severity level.

   The scale of severity level ranges from 0 (the least) to 4 (the most logging done).
5. Click **Ok**.

Note:
For information about changing the logging level for an individual server, see Debug tab on page 70.

Avaya IC Manager log file maintenance

Avaya IC Manager logs do not write over themselves when they get to a certain size. Instead, they continue to grow until you delete the logs or until the logs run out of disk space.

You should use the Windows File Explorer to periodically delete the Avaya IC Manager logs to avoid any problems. The following Avaya IC Manager logs reside in the `IC_INSTALL_DIR\etc\logs` subdirectory:

- `General_<username>.log`
- `CtiNmi.log`
- `Admin.log`.
- `ICManager_<username>.log`

Setting environment information

You can set the Avaya IC environment options and import, export, or reload configuration options by selecting **Manager** > **Options** and clicking the **Environment** tab. The available options are:

Option	Description
Hostname Resolution	By default, Avaya IC Manager performs a host information search on the servers that are running Avaya IC services to convert their IP addresses to hostnames. Systems with an incorrectly configured DNS environment can experience a significant slowdown as Avaya IC Manager tries to resolve the hostname of an IP address. Using this option, you can disable the Hostname resolution process to conserve system resources. To enable or disable the hostname resolution, you have to select or clear this check box.
Timer (minutes)	Determines how frequently Avaya IC Manager performs such activities as server status pings.
Browser	Specifies the browser to be used for Web services. If the default browser on your system is Internet Explorer, you do not need to select a browser in this field. **Note:** From IC 7.3.2 onwards, IE 9 and 10 is supported and it must be launched from a system with 32-bit. From IC 7.3.3 onward, IE 11 is supported and it must be launched from a system with 32-bit.

Option	Description
Import Configuration	Click this button to import a saved XML configuration file. The configuration file contains the settings for the servers in the Avaya IC system. The default file is: `IC_INSTALL_DIR\etc\sc.xml`.
Export Configuration	Click this button to export the current configuration settings in an XML file.

Monitoring alarms

Alarms are messages displayed by Avaya IC. These alarms alert you to unusual situations or provide additional information. When Avaya IC Manager receives an alarm message, it changes the Alarm Monitor icon in the bottom right corner of the main Avaya IC Manager window. It also displays the alarm message besides the icon.

To view alarms and change alarm settings, select **Tools** > **Alarm Monitor**. (If this option is not available, you may not have the correct security privileges. To check your privileges, talk to your Avaya IC administrator.)

Alarms are displayed in reverse chronological order with the most recent alarms displayed at the top in the list. If duplicate alarms are generated, the first column displays the number of times the alarm has been received. (If you want each instance of an alarm to be individually listed, select **Options** > **Filter Duplicates**. Selecting this menu item toggles between the two display modes.)

You can display a subset of alarms by selecting either one or more domains or host systems, systems on which servers are located, to be monitored.

To select domains

1. From the **Alarm Monitor**, select **Alarm** > **Domains**.
2. From the **Available Domains** list, select the domain that you want to add and click **Add**.

   You can add all the domains by clicking **Add All**.
3. To remove a domain, select it in the **Selected Domain** list and click **Delete**.
4. Click **Ok**.

   Avaya IC Manager begins monitoring alarms from only the selected domains.

To remove domains

1. From the **Alarm Monitor**, select **Alarm** > **Domains**.
2. In the **Selected Domain** list, select the domain that you want to remove.
3. Click **Delete**.
4. Click **Ok**.

   Avaya IC Manager begins monitoring alarms from only the selected domains.

To select host systems

1. From the **Alarm Monitor**, select **Alarm** > **Hosts**.
2. Enter the names of the hosts to be monitored and click **Ok**.

If service between Avaya IC Manager and the Alarm servers is interrupted at any time, you must re-synchronize Avaya IC Manager and the Alarm servers by selecting **Alarm** > **Re-monitor**.

To clear the alarms from the Alarm Monitor and reset the Alarm Monitor icon on the main Avaya IC Manager window, select **Alarm** > **Clear Alarms**. To clear just the Alarm Monitor icon, select **Alarm** > **Clear Alarm Button**.

You can set the following preferences from the Options menu:

Filter Duplicates: If selected, the Alarm Monitor displays each alarm only once and provides a counter showing how many times that particular alarm has occurred. If cleared, the Alarm Monitor displays each instance of an alarm individually.

Beep on Alarm: If selected, the Alarm Monitor beeps when an alarm arrives.

Pop Up On Emergencies: If selected, the Alarm Monitor opens automatically when an emergency alarm is received.

Ignore Low Priority Alarms: If selected, the Alarm Monitor does not change the Alarm Monitor icon when a low-level alarm is received.

To raise a test alarm, select **Test** > **Raise Alarms** or **Test** > **Raise Emergency Alarm**.

CIRS alarms

The Central Internet Routing Service (CIRS) servlet is a load-balancing servlet for Web Management. If it is not used, the website cannot find it, so it sends an alarm to Avaya IC Manager. This servlet is used only if you have multiple ICM servers; otherwise, you can safely ignore the alarm. For information on the CIRS servlet, see CIRS record properties on page 139.

Resetting the system time zone on Avaya IC systems

Before you reset the system time zone on any system running Avaya IC Manager or Avaya Agent, you must stop all instances of Avaya IC Manager, the Avaya IC servers, and the Avaya Agent clients. After you finish setting the system time zone, restart your servers and clients so that they synchronize properly with the new time zone setting.

For more information, see Starting or stopping a server on page 78. For more information about working with servers, see Managing servers on page 62.

Tuning and maintaining the Avaya IC database

You should regularly tune and maintain your Avaya IC database to make sure that it runs as efficiently as possible and that it does not take up unnecessary space. For more information, see Appendix A: Database tuning and maintenance on page 394.

Configuring clusters

Avaya IC has provided redundancy support for Email, Poller, and WebACD servers. You can add one additional server for each Email, Poller, and WebACD server.

To achieve redundancy, you need to form a group of two identical servers, which is called as Cluster. For example, you can create an email cluster for two Email servers, or a Poller cluster for two Poller servers.

Each server in a cluster acts as a redundant server to another. One server acts as a primary server and the other acts as secondary server. In each cluster, only one server is active or functional at a time.

CAUTION:
From ICManager, if you try to delete any Poller, Email, or WACD server that is associated with the respective cluster, ICManager displays a warning message. The message states that the Poller server, Email server, or WACD server will be deleted from the corresponding cluster. The warning message also displays name of the cluster and the server details to which the Poller server, Email server, or WACD server belongs.

This section includes the following topics:

- Observations of default email cluster becoming nonfunctional on page 47
- Creating Clusters on page 48
- Editing Clusters on page 49
- Deleting Clusters on page 49
- Mapping clusters on page 50

Observations of default email cluster becoming nonfunctional

In the default email cluster, if the functional email server becomes nonfunctional or the default email cluster becomes nonfunctional, agents can observe the following until any one email server in the default email cluster becomes functional:

- Agents cannot reply to the emails that arrive from the default email cluster.
- Agents cannot send the emails from the default email cluster.
- Agents might continue to receive emails from other email clusters if other email clusters are configured.
- In Avaya Agent Web Client (AAWC), the email channel of agents gets impaired. To successfully perform the email operations, the agent needs to reset the email channel after an email server in the default email cluster becomes functional. For more information about resetting the email channel, see *Avaya Agent Web Client User Guide*.

- In Avaya Agent Rich Client (AARC), the Web Agent status bar displays the status of the email channel with red icon. When an agent tries to send or reply to an email, the email channel icon on the Media tab disables and the email operation fails by displaying the error message. Agent can perform the email operations only when the connection to the functional email server in the default email cluster is restored. Agents must wait until the Web Agent status bar displays the status of the email channel with green icon. For more information about email channel status, see *Avaya Agent User's Guide*.

Creating Clusters

In Avaya IC Manager, you can create separate clusters for Email and Poller servers. While creating a cluster, you need to select the primary server and a secondary server to be included. The system displays an error message appears if there is no email or poller server available to create the corresponding cluster.

- Poller Cluster on page 48
- ICEmail Cluster on page 48

Poller Cluster

It is a cluster of two Poller servers.

To create a poller cluster:

1. In Avaya IC Manager, from the main menu, select **Services** > **Cluster Configuration**.
2. On the toolbar, click **New**.
3. In the **Cluster Name** field, enter the Poller cluster name.
4. In the **Primary Server** field, select the primary server.
5. In the **Secondary Server** field, select the secondary server.
6. Click **Ok**.

ICEmail Cluster

It is a cluster of two Email servers.

To create an IC Email cluster:

1. In Avaya IC Manager, from the main menu, select **Services** > **Cluster Configuration**.
2. Click the **ICEmail** tab.
3. On the toolbar, click **New**.
4. In the **Cluster Name** field, enter the IC Email cluster name.
5. In the **Primary Server** field, select the primary server.
6. In the **Secondary Server** field, select the secondary server.

Note:
The secondary server should be different from the primary server.

7. Click **Ok**.

Editing Clusters

In Avaya IC Manager, you can edit the IC Email, Poller, and WACD clusters. While editing a cluster, you can modify the server, which is currently not running or not functional.

If you want to modify the nonfunctional server to a different server, you must remove the nonfunctional server from the cluster by selecting the **NO SELECTION** option in the corresponding drop-down list and then selecting the new server from the same drop-down list.

To edit a cluster:

1. In Avaya IC Manager, from the main menu, select **Services** > **Cluster Configuration**.
2. On the toolbar, click **Edit**.
3. In the drop-down list, select the **NO SELECTION** option.

   The server is indicated by a red or an orange icon.
4. Click **Ok**.
5. Select the same cluster again.
6. Click **Edit**.
7. In the drop-down list, select the new server.

   The server is indicated by the red icon.
8. Click **Ok**.

Note:
Do not start the IC Poller server, the WACD server, and the IC Email server till they are added to the respective clusters or else, the servers might crash.

Deleting Clusters

In Avaya IC Manager, you can delete only the IC Email and Poller clusters.

To delete a cluster:

1. In Avaya IC Manager, from the main menu, select **Services** > **Cluster Configuration**.
2. Click the tab for the cluster that you want to remove.
3. On the toolbar, click **Delete**.
4. Click **Yes** to confirm.

Mapping clusters

Cluster mapping helps you to map the Poller cluster with IC Email cluster. Mapping these clusters lets the IC Email cluster know from which poller cluster, the emails must be fetched.

Mapping the clusters automatically maps the functional server in each cluster.

Note:
Avaya IC supports mapping of only IC Email and Poller clusters.

To create a new clustermap:

1. In Avaya IC Manager, select **Services** > **Cluster Configuration**.
2. Click the **ClusterMap** tab.
3. Click **New**.
4. From the **Poller Cluster** drop-down list, select poller cluster.
5. From the **IC Email Cluster** drop-down list, select the email cluster.
6. Click **Ok**.

To edit a clustermap:

1. In Avaya IC Manager, from the main menu, select **Services** > **Cluster Configuration**.
2. Click the **ClusterMap** tab.
3. Select the clustermap that you want to edit.
4. Click **Edit**.
5. In the **Poller Cluster** field, select a poller cluster.

   Note:
   After you select the Poller cluster, the **ICEmail Cluster** drop-down list displays all the available email clusters which are not mapped with the poller cluster that you have selected. Instead of editing the poller cluster, you must create a new map.

6. In the **IC Email Cluster** field, select an email cluster.
7. Click **Ok**.

To delete a clustermap:

1. In Avaya IC Manager, from the main menu, select **Services** > **Cluster Configuration**.
2. Click the **ClusterMap** tab.
3. Select the clustermap that you want to delete.
4. Click **Delete**.

Chapter 3: Domains

When a contact enters Avaya Interaction Center (Avaya IC), several servers must interact to handle that contact. Each group of inter-connected servers is called a domain. You can configure domains to accommodate your hardware architecture whether it is located at different sites or on multiple systems at one site. Domains can span servers at different locations and multiple domains can share the same server. For information on creating sites, see Managing sites on page 37.

A failover order is associated with each domain. The failover order defines how the members of a domain failovers to servers in other domains. In multi-site organizations, you can set up domains on the different sites. If a server becomes unavailable on one site, the requests to that server are routed to a server in the failover domain on the second site. For details about deploying Avaya IC on you domain, see *IC Installation Planning and Prerequisites*.

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 or system performance will be adversely affected.

After creating your domains, you assign agents to those domains to determine which group of servers will service their requests.

For example, you can set up a primary domain on your main server with a secondary domain on your backup server. If there is a problem with a server in the primary domain, it can failover to the secondary server without disrupting service.

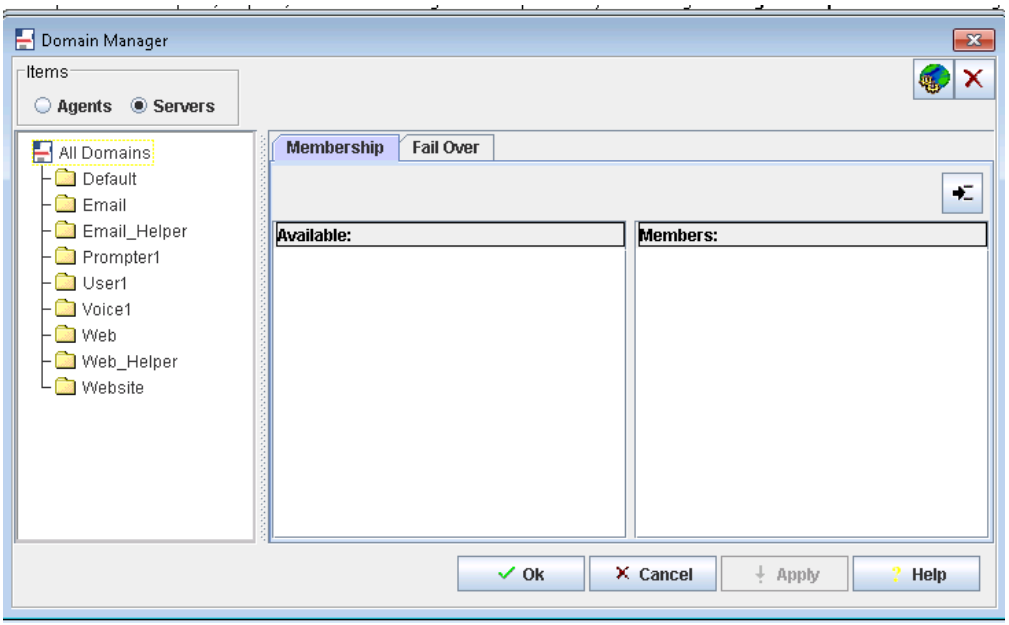
Avaya IC is a highly configurable environment that gives you flexibility in defining the server to server and client to server communication flow. Avaya IC servers are location independent and can be hosted either on the same system, or across multiple systems. Domains can be used to help partition servers into functional services that process Chat, Email, and Voice contacts. This allows you to increase the performance of your Avaya IC system and enable it to handle higher contact rates.

Using the Workflow server as an example:

- Instantiating multiple Workflow servers to run on different systems helps to increase the number of contacts that your contact center can handle.
- Dividing the routing, blending, and application support across multiple servers increases the bandwidth of Avaya IC to handle more contacts.

You may also want to perform workflow routing and task blending by the individual channels. You can set up domains to contain their own EDU and Workflow servers designed to handle contacts from voice, email, and chat channels.

The following figure shows the Domain Manager window:



This section contains the following topics:

- Setting up your domains on page 53
- Creating your domains on page 54
- Assigning servers to a domain on page 55
- Creating failover domains on page 56
- Assigning agents to the domains on page 61

Setting up your domains

While you are deciding on the domains that you need in your Avaya IC environment, you must consider the following points:

- You must use logical names that include your site name, the name of the workgroup of the agents, or the type of channel.
- All servers and agents need to communicate with the core servers, so you must install the core servers on a system that is easily accessible from everywhere within Avaya IC.

- You must include at least an ORB server, an Alarm server, and a Directory server either in the domain itself or in an associated failover domain. If these servers do not exist, then Avaya Agent will not function correctly. Servers and agents needs to find ORB/Directory/Alarm in their failover list.
- Agents and servers must belong to one, and only one, domain. If you add an agent or server to a second domain, Avaya IC Manager automatically deletes that agent or server from the first domain.
- Domains must not contain multiple servers of the same type, with the possible exception of the ORB server. You can have multiple ORB servers in the same domain if those ORB servers all reside on different physical devices.

After you have decided on the domains you need in your Avaya IC configuration, follow the steps in:

- Creating your domains on page 54.
- Assigning servers to a domain on page 55.
- Creating failover domains on page 56.
- Assigning agents to the domains on page 61.

Creating your domains

The installation procedure creates a complete domain structure named Default. An instance of each of the Avaya IC core servers is placed in the domain. You can use or modify this structure as required. The installation creates other domains as well but those domains do not have servers configured for them.

Note:
Avaya IC requires that the Default domain remain in the system. You can create additional domains for your contact center, but you cannot delete the Default domain.

To create a new domain

1. In Avaya IC Manager, click the **Domain** button on the toolbar.

   The **Domain Manager** opens.
2. In the **Items** section, select **Servers**.
3. Click **New**.
4. Enter the name of the new domain.

   The domain name can be maximum of 32 characters including underscore. Spaces are not allowed in the domain name. The domain name must start with an alphabetic character.
5. Click **Ok**.

   The new domain name is added in the **All Domains** list in the left pane of **Domain Manager**.

6. If you are running multiple instances of Avaya IC Manager to administer Avaya IC, select **Manager** > **Refresh** on each instance of Avaya IC Manager to make each instance of Avaya IC Manager aware of the changes.

Assigning servers to a domain

By default, servers are assigned to the Default domain when they are created, but you might want to assign the servers to a different domain. You can assign any number of servers to a domain, but you should not include multiple servers of the same type or there could be confusion during the failover process. This is especially important if you want all of the clients to communicate with the same server. The only exceptions to this rule are the ORB server, the Attribute, and Workflow servers because these servers do not failover.

Each server name must be unique, as the same server cannot exist in multiple domains. For instructions on creating servers, see Creating a server on page 74. For deployment scenarios, see *IC Installation Planning and Prerequisites*.

To assign servers to domains:

1. In Avaya IC Manager, click the **Domain** button on the toolbar.

   The **Domain Manager** opens.
2. In the **Items** section, select **Servers**.
3. In the left pane, select the name of the domain to which you want to add servers.
4. In the right pane, select a server from the **Available** list that you want to add to the selected domain.
5. Click **Add** to move the selected server to the **Members** list.
6. Click **OK** after you have assigned all required servers to the domain.
7. If you are running multiple instances of Avaya IC Manager to administer Avaya IC, select **Manager** > **Refresh** on each instance of Avaya IC Manager to make each instance of Avaya IC Manager aware of the changes.

Note:
A server must belong to a domain. Therefore, if you want take a server out of a particular domain, you must move that server into a different domain or delete the entire server.

Creating failover domains

If a server becomes unavailable during operation, the server's client's requests are redirected to an alternative server. The client is said to have failed over to the alternate server. This client can be either an agent's desktop application or another server.

A client or server logs in to the IC system by a request to the Directory server. If there is no information available to identify the domain of the client or domain of the server making the request when the request is invoked, we assume that the requester is in the Default group.

While membership in a domain determines how the domain members communicate with servers, membership also defines how failover is performed for all servers. Failover domains must be added to the appropriate failover lists because only servers in failover domains can be reached by servers in different domains.

Before proceeding further, carefully plan your server failover strategy. For more information, see *IC Installation Planning and Prerequisites*.

To establish the failover order for a domain:

1. In Avaya IC Manager, click the **Domain** button on the toolbar.

   The system displays the **Domain Manager** window.
2. In the **Items** section, select **Servers**.
3. In the left pane, select the domain for which you want to specify the failover order.
4. In the right pane, click the **Failover** tab.
5. Select the backup domain from the list in the **Available** pane.
6. Click **Add** to move the backup domain into the **Members** pane. If you specify multiple domains to be used for failover, they will be used in the order specified. Use the **Up Arrow** and **Down Arrow** buttons located above the **Members** list to rearrange failover order, making sure you do not move any of the failover domains before the primary domain.

   Note:
   Failover order can also be set on a server-by-server basis. For details, see Advanced tab on page 73.
7. Click **Ok**.
8. If you are running multiple instances of Avaya IC Manager to administer Avaya IC, select **Manager** > **Refresh** to make this instance of Avaya IC Manager aware of the changes.

Preconfigured Failover Domains

Avaya IC includes several domains that are preconfigured with failover paths. The following table describes the preconfigured domains. For details about the appropriate configuration for your site, see the deployment scenarios in *IC Installation Planning and Prerequisites*.

Preconfigured domain	Members	Failover path
Default	• Alarm server • Directory server • License server • ORB server • JavaAppBridge server	• Default
Core2	None	• Core2 • Default
Email	None	• Email • Email_Helper • Default • Core2 **Note:** In case you modify the Analyze Workflow to access the ADU server, you need to modify Email domain failover sequence to have a domain that has an ADU server.
Email_Helper	None	• Email_Helper • Default • Core2
Email2_Helper	None	• Email2_Helper • Default • Core2

Preconfigured domain	Members	Failover path
Prompter1	None	• Prompter1 • Prompter2 • Default • Core2 • Voice1 • Voice1_Helper • Voice2 • Voice2_Helper
Prompter2	None	• Prompter2 • Prompter1 • Core2 • Default • Voice2 • Voice2_Helper • Voice1 • Voice1_Helper
User1	None	• User1 • User2 • Prompter1 • Prompter2 • Default • Core2 • Voice1 • Voice1_Helper • Voice2 • Voice2_Helper • Email • Email2 • Email_Helper • Email2_Helper • Web • Web_Helper • Web2 • Web2_Helper

Preconfigured domain	Members	Failover path
User2	None	• User2 • User1 • Prompter2 • Prompter1 • Core2 • Default • Voice2 • Voice2_Helper • Voice1 • Voice1_Helper • Email • Email2 • Email_Helper • Email2_Helper • Web • Web_Helper • Web2 • Web2_Helper
Voice1	None	• Voice1 • Voice1_Helper • Voice2 • Voice2_Helper • Core2 • Default
Voice1_Helper	None	• Voice1_Helper • Voice2_Helper • Core2 • Default
Voice2	None	• Voice2 • Voice2_Helper • Voice1 • Voice1_Helper • Core2 • Default

Preconfigured domain	Members	Failover path
Voice2_Helper	None	• Voice2_Helper • Voice1_Helper • Core2 • Default
Web	None	• Web • Web_Helper • Default • Core2 Note: If you do not configure the Event Collector server to monitor the ADU server in this domain, configure the server groups on the Advanced tab as follows: Web: Priority Value = 1
Web2	None	• Web2 • Web2_Helper • Default • Core2 **Note:** If you do not configure the Event Collector server to monitor the ADU server in this domain, configure the server groups on the Advanced tab as follows: Web: Priority Value = 1
Web_Helper	None	• Web_Helper • Default • Core2
Web2_Helper	None	• Web2_Helper • Default • Core2
Website	None	• Website • Web • Voice1 • Voice1_Helper • Default • Core2

Assigning agents to the domains

Agents are assigned to domains based on the services they are accessing and their network location relative to those services. You can use domains to distribute agents across multiple IC servers to achieve horizontal scalability. You can use the Domain Manager to assign agents to domains, but the preferred method is to specify the agent's domain when you create the agent in the Agent Editor. You must specify a domain when you create the agent record. For instructions, see Membership information on page 222.

Each agent can be assigned to only one domain. If you add an agent to a second domain, Avaya IC Manager deletes that agent from the first domain.

To assign agents to domains:

1. In the **Domain Manager**, select **Agents** in the **Items** box at the top of the window.
2. Select the name of the domain to which you want to assign the agents. The agents that you can assign to the domain are listed in the Available pane and the agents that are already assigned to the domain are listed in the Members pane.
3. Select an agent from the **Available** pane.
4. Click **Add** to move the agent to the **Members** list for the selected domain.

   Note:
   You can select multiple agents by pressing **Shift** while selecting a contiguous set of agents, or pressing **Ctrl** while selecting a non-contiguous set of agents. To remove an agent from a domain, you must assign the agent to a new domain. The agent is then automatically removed from the previous domain.

5. Click **OK**.

   This adds an agent to the domain and updates the database.

Chapter 4: Managing servers

In Avaya IC Manager you can add servers to Avaya Interaction Center (Avaya IC), view or modify server information, assign servers to domains, and perform other management tasks based on the security level assigned to you.

To display the **Server Manager**, click the **Server** tab in the Avaya IC Manager window. The left pane of the **Server Manager** lists the domains that have been created in Avaya IC. For instructions on adding domains to Avaya IC, see Creating your domains on page 54.

To view:

- all available servers, select **All Domains** in the left pane.
- the servers in a single domain, select that domain in the left pane.

Tip:
When the **Server Manager** is initially displayed, **All Domains** is selected by default. To improve start-up performance, disable the **Auto Load** option on the **Server** menu. If **Auto Load** is disabled, you must select a specific domain to view the servers in that domain.

The right pane of the **Server Manager** contains a table that displays the following information about each server:

Field	Description
Type	The type of the server.
Name	The name of the server. Naming servers eliminates confusion when multiple servers of the same type are installed. To prevent any confusion, keep the server name different from the interface name.
Domain	The domain name of the server. A domain is a set of servers that respond to requests from clients. (For details, see Creating your domains on page 54.) The membership of a server to a domain defines how it will communicate with other servers.
Status	The status of the server can be Up or Down. To view the status, select the server and select **Status** in the toolbar. If the **Auto Update** option is enabled in the **Server** menu, the status column is updated automatically. However, this option is not recommended for large contact centers. The Advanced status information, which is not updated automatically, is available from the **Advanced** tab of **Server Editor**.

Field	Description
Host	The system on which the server is installed. By default the IP address is used unless you enable hostname resolution in the **Options** dialog of Avaya IC Manager.
Port	The port number being used by this server to communicate with clients and other servers. For a list of default port numbers for components in Avaya IC, see IC Installation and Configuration.
Uptime	The period of time since this server was last started.

To sort the list of servers in ascending order, click on a column header. To sort the list of servers in a descending order, hold **Shift** and click the column header. To automatically sort the list by the first column, select **Server** > **Auto Sort**.

To change the size of the columns, click between the column headings and drag the black line to the desired size.

This section contains the following topics:

- Server overview on page 64
- Changing server information on page 67
- Creating a server on page 74
- Determining server start up or shutdown dependencies on page 75
- Updating server information on page 79
- Copying or moving a server on page 79
- Deleting servers on page 79
- Synchronizing multiple Directory servers on page 80
- Configuring Web Management servers on page 81
- Enabling the SSL security for the Directory server on page 87
- Enabling the SSL security for the HTTPConnector server on page 88

Server overview

Avaya IC is made up of servers that interact with each other to provide its functionality. The following table describes the out-of-the-box Avaya IC servers:

Server Name	Description
ADU server	Holds up-to-date information on all active agent and queue data units in the Avaya IC system. If you are using Business Advocate, this server also contains statistics for the Business Advocate service classes.
Alarm server	Receives and propagates alarms to interested clients. It is used to notify problems to the interested clients or send informational messages. Also sends SNMP traps to the configured trap sinks if SNMP is enabled.
Attribute server	Acts as a communications bridge between the ICM server and the WebACD server for chats. Provides tracking of user web page browsing sessions for DataWake. This server also provides website property event notifications between the website and the ICM server. (For details on the ICM server, see ICM record properties on page 140.)
Blender server	Controls agent availability across the different channel types and monitors ADU change events. It can be configured to run blending flows when any agent state changes. The Blender server can also be configured to raise alarms or run flows when agent or queue ADU thresholds are exceeded.
CAServer (Content Analyzer) server	Handles runtime language determination and analysis of text within an email in conjunction with the IC Email server. Each CAServer is configured to open one or more knowledge bases built with Content Analyzer. For details, see Chapter 7: Using Content Analyzer for automated email processing on page 170.
CAAdmin server	Handles administrative requests for the optional Content Analyzer feature of Avaya IC. The CAAdmin server supports the creation, training, validation, and saving of Knowledge Bases. After the Knowledge Bases are created using this process, they are ready for use by the production Content Analyzer server (CAServer).
ComHub server	Assists in passing administration information to the WebACD server from a web-based interface. It also helps the WebACD server respond to agent request such as logon or logoff.
Data servers	Permit Avaya IC clients and servers access to a database server regardless of the database type, using only their Avaya IC accounts. All Data servers support connection pooling. There are five types of Data servers that handle DB2, Data, ODBC, Oracle, and SQL server connections.

Server Name	Description
Directory server	Looks up the agent, workgroup, queue, tenant, and server configuration information for other servers in the Avaya IC system. In addition, Avaya IC Manager uses the Directory server for administrative purposes.
DUStore server (Data Unit persistent Store)	Serves as the backup store for the data unit servers (ADU, EDU) by letting idle data units be pushed out of memory to make room for active data units. It is used in cases of failure recovery because it allows data units to persist across server shutdowns.
EAI servers	The EAI server, EAI Email server, and EAI Workflow server are used when you integrate Siebel 8 with Avaya IC. For details, see *Avaya IC for Siebel 8 Integration*.
EDU (Electronic Data Unit) server	Maintains all active Electronic Data Units (EDUs). Each data unit represents a contact (chat, email, voice) in the Avaya IC system. This server is used by all channel servers and clients to keep track of and update contact information.
Event Collector server	Collects events published by the Avaya IC ADU and Directory servers. These events contain data representing state changes impacting Agents, Queues, and associated administrative data that supports Avaya OA real time and historical reporting. For details, see the *Operational Analyst Installation and Maintenance Guide*.
Event Collector bridge	Functions as a gateway between the Event Collector server and Business Advocate. This server queries Business Advocate data and collects Business Advocate administration events that are published to Microsoft Message Queuing (MSMQ) by Business Advocate. The server sends this data to the Event Collector server, which forwards the data to the Avaya OA Real-time subsystem to support real-time and historical reporting requirements.
HTTP Connector server	Permits Avaya IC server requests to be made as HTTP requests and serves Prompter pages. This server also handles customer account management and authentication for Web Self-Service. This server is a generic HTTP interface server.
IC Email server	The IC Email server interacts with Poller and SMTP servers for polling and forwarding of emails into the Avaya IC system from customer to agent. The IC Email server also manages traffic flow to Subject Matter Experts and Approval agents. The Poller server does not poll emails that do not have the FROM, and REPLY-TO header. Such emails are skipped by the Poller server and the exchange admin must clean up these mails. The IC Email server works closely with workflows to accomplish these goals.
JavaAppBridge server	Allows the Avaya Agent Web Client or SDK application to communicate with IC servers.

Server Name	Description
License server	Ensures that the features and agents that have been purchased can be run. It communicates with each of the installed Web License Manager components.
Notification server	Allows Avaya IC components to schedule events (the delivery of email, faxes, messages, or alerts) in the future, either specifically by an agent or based on escalation and action rules. The Notification server provides email lifecycle support by alerting agents to potential delays in email processing.
ORB server	Oversees and starts the other Avaya IC servers. Any host system that is to run Avaya IC servers must have an ORB server installed and running.
Paging server	Serves as a communications bridge between Avaya Agent and the WebACD server. This server brokers messages so they get sent to the proper agents and WebACD server.
Poller server	Interacts with POP3, and IMAP4 servers to poll emails from the exchange server that you have configured. The Poller server stores the polled emails in the IC CCQ database.
Report server	Records data unit information for the EDU and ADU servers. The reporting tools use this information to generate historical reports. When Avaya IC terminates an EDU or ADU, the data unit is passed to the Report server. This server may run mapping rules to convert an EDU into the appropriate format for reporting. The Report server writes its information into the IC Repository database.
Resource Manager server	Matches agents to contacts in a Business Advocate environment.
Siebel AICD (Adaptive Interaction Center Driver) server	This server is used when you integrate Siebel 8 with Avaya IC and is used to pass work-related information, such as commands and events, between Avaya IC and Siebel. For details, see *Avaya IC for Siebel 8 Integration*.
Siebel - Agent Server for Integration with Siebel (ASIS) server	This server handles requests and event communication for all agents and is used instead of the Avaya Agent application for Avaya IC for Native Siebel configurations. For details, see *Avaya IC for Siebel 8 Integration*.
Siebel EAI (Enterprise Application Integration) servers	The EAI server, EAI Email server, and EAI Workflow servers are used when you integrate Siebel 8 with Avaya IC. The Avaya EAI servers provide the communication links between Avaya IC and Siebel so that Avaya IC workflows can read and write customer data. For details, see *Avaya IC for Siebel 8 Integration*.
TS (Telephony) server	Serves as the connector server for the voice channel. It interfaces with a PBX and monitors phone calls and control routing of telephony requests. It uses the EDU server to record information on incoming or outgoing phone calls. (Also called the Voice Connector server.)

Server Name	Description
TS Queue Statistics	Monitors the telephony channel and keeps up-to-date queue statistics in the ADU server (such as contact count and age of oldest contact).
TSA (Telephony Services Adaptor) server	Manages server interactions for Business Advocate that are required for voice contacts. Business Advocate requires a TSA server for every switch in your Avaya IC system.
VOX server	Interfaces with Interactive Voice Response units (IVRs). It provides the IVR with the ability to make Telephony server and EDU calls.
Web Advocate Adaptor (WAA) server	Manages server interactions for Business Advocate that are required for chat contacts and email contacts.
WebACD (Web Automatic Call Distributor) server Also called: WACD	The Call distributor for chats and emails. This server is responsible for assigning tasks to agents and tracking the different states such interactions undergo. It makes use of the Attribute, Paging, IC EMail and ComHub servers to complete support operations such as managing agent logon/logout states and the actual administration of the interactions.
Web Scheduled Callback server	Schedules callbacks requested from a public website. Creates a chat and a callback task at the scheduled time.
Workflow server	Processes workflows that route contacts and implement business rules. The Workflow server can handle specific tasks, such as media routing, agent blending, agent scripts, letter generation, and generic business logic. Workflows can be run by direct invocation or as a result of receiving events from another server. You can distribute these responsibilities across multiple Workflow servers to maximize performance and response from the server. For example, if your Avaya IC system includes multiple server machines, you can install secondary Workflow servers dedicated to specific media contacts on the secondary machines.

Changing server information

The Avaya IC Directory Server stores certain information about servers, such as their names, locations, and configuration settings. Sometimes it is necessary to change this information. For example, certain configuration parameters must be set when servers are installed.

To change information about a server, double-click the server name from the list on the Server Manager in the Avaya IC Manager window. Avaya IC Manager displays the **Edit Server** window.

The tabs displayed in the **Edit Server** window vary depending on your security level. To view all of the tabs, you must be logged in with Administrator credentials. The options for each tab are described in the following sections.

Note:
For detailed server deployment guidelines, see *IC Installation Planning and Prerequisites*.

This section contains the following topics:

- General tab on page 68
- Server tab on page 69
- Configuration tab on page 70
- Debug tab on page 70
- Advanced tab on page 73

General tab

The General tab displays information about the server's location and status. This information is placed in the directory when the server is installed and should not be altered.

Name: The server name can be up to 32 characters long (without spaces) and must be unique. Avaya recommends that:

- You should name your Data servers Data_<*databasetype*>_<*domain*>. For example, **Data_Oracle_Default**.
- In a single site environment, you should name all other servers <*servername*>_<*domainname*>. For example: **ADU_User1**.
- In a multi-site environment, you should name all other servers <*servername*>_<*sitename*>_<*domainname*>. For example: **ADU_London_User1**.
- Do not set the server name same as the server type. Avaya IC may encounter errors during operation. For example, use **TS_Voice1** as the name of your Telephony server, not only **TS**.

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

Domain: The domain to which the server belongs. You can change the assignment of a server to a domain on this tab.

Host: The name of the host system on which the server resides. Select a name from the drop-down list. It lists all systems in the network that contain an ORB server, or enter another system name.

Once the name, domain, and host are selected, the following three fields are filled in automatically, which can be changed if needed:

Directory: The directory in which the `vesp.imp` and the `ds.ffd` files are located (default: `IC_INSTALL_DIR\etc`)

Port: The port number being used by the server to communicate with clients (default: the next available number). For a list of default port numbers for components in Avaya IC, see *IC Installation Planning and Prerequisites*.

Executable: The path to the server executable file (default: *`IC_INSTALL_DIR\bin`*)

> **Note:**
> If you are adding a data server, you do not need to complete this field. It will be filled in automatically.

Auto Start: Select Autostart if ORB should automatically and immediately restart the server if the server fails or abnormally terminates for any reason. ORB starts that server when the ORB itself starts up. For example, at system start up. Enabling Autostart on a server does not restart the server if it is shutdown from Avaya IC Manager. The server will automatically start if there is request from the client or other servers. (This option is disabled for ORB servers.) Avaya recommends that you manually start the server to validate its configuration before enabling the Autostart option.

Security: Select Security to give the server security privileges. This allows the server to write to the Directory server, which is essential for some operations.

The third section provides information about the server's status that Avaya IC Manager refreshes automatically. This information cannot be modified.

Server tab

If there are any options or configuration parameters specific to the type of server you are creating or editing, Avaya IC Manager displays those options on a server specific tab in the Server Editor. Avaya IC Manager provides default values for most of these options when the server is first installed, and you should use caution when modifying these values.

The server specific configuration parameters for all of the standard Avaya IC servers are described in Appendix C: Server configuration reference on page 418.

When you click **OK** or **Apply**, Avaya IC Manager checks values to ensure that they do not violate any restrictions, such as a minimum or maximum value.

> **Note:**
> If you modify configuration parameters, you must stop and restart the server for the new settings to take effect. For instructions, see Determining server start up or shutdown dependencies on page 75.

Configuration tab

Configuration parameters are additional instructions that Avaya IC Manager runs when a server starts. You set the configuration parameters for the Avaya IC servers on the server specific tab, but parameters for custom servers can be entered on the Configuration tab.

CAUTION:
You should enter data only for the standard Avaya IC servers on the Configuration tab under the direction of Avaya Technical Support. Avaya IC Manager does not do any error checking on the parameters entered on this tab.

To add a configuration parameter:

1. In **Server Editor**, click the **Configuration** tab.
2. On the toolbar, click the **New** button.

   Avaya IC Manager displays the **CTI Type Editor**.
3. From the **CTI Type** drop-down list, select the format of the parameter:
   - **Couple** (containing a name and a value).
   - **Sequence** (containing a comma-separated list of couples).
4. In the **Name** field, enter the name of the field to which you are adding the parameter.
5. In the **Value** field, enter the value to be stored in the directory.
6. Click **OK**.

Note:
If you modify configuration parameters, you must stop and restart the server for the new settings to take effect.

Debug tab

Occasionally, problems may arise in the Avaya IC system. To assist in diagnosing problems, each Avaya IC server creates a log file containing information about the activity of the server. The amount of information written to a log file of a server and the maximum size of the log file are established on the Debug tab. (The type of server determines what debug parameters are available on this tab.)

CAUTION:
You should only change the settings on this tab under the direction of Avaya Technical Support because writing excess information to log files can degrade the performance of the system.

The log files are named as server name with an extension `log`.

The common debug parameters are:

Parameter	Description
Data Query Log Level	Select a number from 0 to 3, where 0 is the lowest level of logging and 3 is the highest. Because logging requires system resources, you should select a minimal logging level unless you are trying to diagnose a specific problem.
Log File Size	Enter the maximum size of the log file. The default log file size is 25 MB (25,600,000 bytes). The minimum is 1000 bytes and the maximum is 50,000,000 bytes. **Note:** After installing Avaya IC 7.3.3 and later, the default log file size of 25 MB is only set to the new servers that you create in IC Manager. For the existing configured servers, the log file size does not change.
Log File Count	Determines the number of log files to retain. The default log files count is 5. **Note:** After installing Avaya IC 7.3.3 and later, the default log file count 5 is only set to the new servers that you create in IC Manager. For the existing configured servers, the log file count does not change.
Log Day Count	Determines the number of days to retain old log files.
Ping Interval (sec)	Enter the number of seconds between messages that are sent to a server to determine if it is running. The minimum is 1 second. **Note:** Ping Interval must be at least twice as long as Ping Timeout. If you enter a value that is less than twice Ping Timeout, Avaya IC will ignore that value and use (Ping Timeout)*2 for the Ping Interval.
Ping Timeout (sec)	The length of time that Avaya IC should wait for a response from the server before determining that the server has failed.
Trace Levels	Click the **Ellipses (...)** and select the required elements.
System Log Trace Levels	Logs the server events. Select a trace level from 0 to 10, where 0 is the lowest trace level and 10 is the highest trace level.

The available trace elements are:

Trace Level	Description
explain	Records detailed messages about the failover decisions that the Avaya IC servers make.
flush	When anything is written to the log buffer, it is immediately written to the log file, rather than waiting for the buffer to fill before flushing to the log file. (This slows the system dramatically. It should be used only for development.)
heap	Turns on additional memory checking. This slows system performance dramatically. This is a deprecated interface that is not supported on all servers.
idl	Higher level trace that is more human-readable than msg. All method invocations are written to the corresponding log file.
mem	Trace all vesp_calloc and vesp_free calls.
msg	Higher level message trace that is used primarily for debugging.
shiptime	Records when a request was actually sent out.
tfunc	For timed functions, print text string and information about what happened whenever the timer goes off.
timing	Measures the time a method request takes.
usr1-usr8	User definable trace levels (get and set trace level functions).

If trace levels are modified, click **Ok** or **Apply**. If the server is running, you are asked if this change should be applied immediately. The ensuing message box asks you if you want these trace levels to be effective on future server restarts.

- Click **Yes** to make the changes permanent.
- Click **No** to make changes for this login session only.

Note:
If debugging is required from Avaya Technical Support, the `idl` and `flush` trace levels should be checked. Be advised that enabling the debugging functionality can reduce system capacity.

Other debug parameters may appear on this tab depending on what server you are working with. For a description of the server specific debug variables, see Appendix C: Server configuration reference on page 418.

Advanced tab

The Advanced tab for all servers contains:

Heap, Cache, and Network buttons: Heap, Cache, Network are deprecated interfaces that are not supported on all servers. When you select one of the buttons, Avaya IC Manager writes the heap, cache, or network information corresponding to a server to a log file of that server.

Important:
These buttons should be used only under the direction of Avaya Technical Support.

Server Status button: Use this option to view a dialog box with server specific information such as the refresh interval for this dialog box and the server's UUID. If the server has shut down, leftover data from the last status request may be displayed. The refresh interval should not be less than 10 seconds to prevent excess server load.

Server Group button: Use this option to override the domain failover policy for any server except for the CAAdmin server. When you set up server groups, failover is done on a server-by-server basis instead of on a domain-by-domain basis. To set up server groups:

1. On the **Server** tab of Avaya IC Manager, double-click on the server that you want to use as the failover server for other servers in this group.
2. On the **Advanced** tab of the Server Editor dialog box, click the **Ellipsis** (**…**) button next to **Server Group**.
3. In the **Server Groups** dialog box, click **New**.
4. In the **CTI Type Editor** dialog box:
   a. In the **Name** field, enter the domain name of the servers that you want to failover to this server.
   b. In the **Value** field, enter one of the following numbers to identify the priority of the domain:
      - **1** for a higher priority domain
      - **2** for a lower priority domain
   c. Click **Ok**.

   Repeat these steps for each domain that needs to failover to this server.
5. In the **Server Groups** dialog box, click **OK**.
6. Click **Ok**.
7. Click **Ok** to close the Server Editor.

Note:
For information about creating a failover mechanism for domains, see Creating failover domains on page 56.

ENV field: Lets you specify server specific environment variables in the format `variable_name=value` (the variable name and value are case-sensitive).

Creating a server

The following procedure does not actually install an executable on the server system. The new server executable and any required files must first be installed as described in IC Installation and Configuration.

In most cases, you can create several instances of a particular server and assign them to different domains so that they can failover in a predetermined pattern, as described in Assigning servers to a domain on page 55. However, before you add your servers to your domains, make sure you examine the deployment information in *IC Installation Planning and Prerequisites*.

To add a new server

1. In Avaya IC Manager, click the **Server** tab
2. On the toolbar, click the **Create Server** button.
3. Select the server type for a standard Avaya IC server.

   Avaya IC uses the server type as the interface identifier when a request is sent to this server.

   Note:
   If you enter your own server type, Avaya IC treats it as a custom server. The description of the server must exist in the IDL for Avaya IC Manager to recognize it. (For details on the IDL, contact Avaya Technical Support.) In addition, the Voice channel configuration property `autoloadint` must be set to True. For more information, see Voice/Configuration property descriptions on page 646.

   Avaya IC Manager displays the **Edit Server** window. Enter server information as described in Changing server information on page 67.
4. Click **OK** to add the server to the list of servers. All of the ORB servers in the directory are automatically updated to include the new server.
5. Select **Server** > **Update** to ensure that all servers are aware of the changes.
6. If you are running multiple instances of Avaya IC Manager to administer Avaya IC, select **Manager** > **Refresh** to make this instance of Avaya IC Manager aware of the changes.

When you create servers, note the following:

- Do not add more than one ORB server per host system.
- If an ORB server has been installed via a secondary install (as described in IC Installation and Configuration), you must exit and log back in to Avaya IC Manager to make Avaya IC Manager aware of the new ORB server. Be sure to select the correct domain.
- Do not add more than one Directory sever per host system. (For details about the Directory server, see the *Core Services Programmer Guide*.)

Determining server start up or shutdown dependencies

Starting and stopping servers in Avaya IC is a simple process. However, you should exercise caution because starting or stopping Avaya IC processes in the wrong order can lead to data loss or system errors. In addition, if your Avaya 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 Avaya IC services.

This section contains the following topics:

- Server startup dependencies on page 75
- IC Shutdown Dependencies on page 76
- Starting or stopping a server on page 78

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 start up time required for each server depends on factors, such as user population, the number of queued emails, and database size. If your servers are taking a long time to start, you can try to reduce the sever load by adjusting some of these dependencies.

To view the state of each server, use the Alarm Monitor in Avaya IC Manager. As servers are started, that server's state will change to **Up** and ORB server sends informational messages to the Alarm Monitor.

Note:
If Avaya IC Manager is running and the Alarm server should fail, Avaya IC prompts the administrator to re-monitor alarms immediately.

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

Note:
From IC 7.3.2 onwards, the Tomcat version supported will be 6.0.37.

Avaya IC uses the following Web Server plugins:

WebAdmin: Required for serving WACD admin pages

Datawake: Captures DataWake information

Jakarta Plugin: Connector between Tomcat and the Web Server

These plugins are available on IIS, Oracle iPlanet and IBM HTTP Server.

The VOX server interfaces with an IVR (Interactive Voice Response) Unit. If the VOX server connects to an external IVR, you should start the IVR first. The VOX server will attempt 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. (For details, see VOX server on page 531.) If the IVR connects to the VOX server, the VOX server must be started first.

If you are using Avaya Operational Analyst, you should always start the Avaya IC components (including all servers and services) before you start the Avaya OA components.

The JavaAppBridge cannot be started or stopped from Avaya IC Manager. The JavaAppBridge is started when the Avaya Agent Web Client application server starts.

IC Shutdown Dependencies

Common reasons for stopping an Avaya IC service include:

- Upgrading to a new version
- Performing regular maintenance
- Changing configuration

Important:
Shutting down any Avaya IC 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 you stop a server used by a client and failover is configured, the clients should fail over 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 Avaya 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 Avaya IC service, you should:

- Do so during a scheduled maintenance period where clients are shutdown and incoming activity can be curtailed.
- Use Avaya IC Manager's Server Shutdown facility in order to ensure the correct communication flow between Avaya IC components, all Avaya IC clients, and the services at the site that should be stopped. The Server Shutdown facility ensures that all Avaya IC processes on that machine are shutdown in the correct order. It does not shutdown dependent Avaya IC processes located on other machines. To use this facility:

1. In Avaya IC Manager, click the **Server** tab.
2. Select **Server** > **Shutdown**.
3. At the prompt, specify the host whose servers you want to shut down. Avaya IC stops all of the servers on the selected host in the appropriate order.

Before stopping the services on a system, you need to consider the impact it will have. Other dependent clients (both agent clients and Avaya IC processes) may need to be shutdown first.

To confirm that an Avaya IC process has shutdown properly, use the System Administration tools provided with your operating system to verify that the process is no longer active. Avaya 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.

Avaya IC processes should be restarted as soon as practical in order to minimize the impact on clients. In many cases, the processes restarts automatically when the system comes back up, or when client requests trigger the server to restart.

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

If you need to shut down individual Avaya IC servers, it is vital that you follow the correct shutdown order to prevent data loss. Stopping a server results in a disruption of the services provided by that server. The following list reflects the impacts beyond the immediate services provided by the server:

Server	Impact
Alarm	This 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 access the database.

Server	Impact
DUStore	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. (For details about data unit persistency, see ADU (Agent Data Unit) server on page 420 and EDU (Electronic Data Unit) server on page 460.)
Event Collector	Without the Event Collector, real time statistics will not be collected by OA for the associated domain.
ORB server	This server is responsible for process management. If the ORB server is not running, no other Avaya IC server can start.

Starting or stopping a server

To start the ORB server, you must use the `icadmin` utility. You can either run `icadmin so` from the command line of the ORB server's host system, or you can run `icadmin so <hostname>` if your host has multiple network interface cards. (For details, navigate to the Avaya IC `bin` directory and enter `icadmin help` on the command line.)

To start or stop any other server

1. In Avaya IC Manager, click the **Server** tab.
2. In the right pane, select the server from the list of servers.
3. On the toolbar, click **Start Server** or **Stop Server** buttons.

Avaya IC Manager lets you start multiple servers at the same time, but you can stop only one server at a time. The Status column displays the updated status of the server. If the system cannot start a server, Avaya IC Manager displays an alarm message.

To stop all Avaya IC servers on one or more systems that have an ORB server installed

1. In Avaya IC Manager, select **Server** > **Shutdown**.

   Avaya IC Manager displays the **Shutdown** dialog box listing all of the systems on which an ORB server is installed.
2. Select the IP addresses (or host names, depending on your system configuration options) of the systems whose servers you want to shut down.
3. Click **OK**.

   Avaya IC Manager shuts down all of the servers on the selected systems.

You can also use the `icadmin` utility to shut down any server. For details, navigate to the Avaya IC `bin` directory and enter `icadmin help` on the command line.

Updating server information

When server information is changed, the changes must be reflected in three areas before they take effect:

- For configuration changes to take effect, the server that was changed must be stopped and restarted. Use **Start Server** and **Stop Server** buttons on the toolbar to start and stop servers.
- Avaya IC Manager automatically updates the directory if the **Auto Commit** option is enabled on the **Server** menu. If this option is not enabled, select **Server** > **Commit** to save changes to the directory.
- If multiple instances of Avaya IC Manager are used for concurrent administration, select **Manager** > **Refresh** to update the server and domain information and make all instances of Avaya IC Manager aware of the changes.
- To force the update of all ORB servers, select **Manager** > **Update ORB Servers**. This propagates all server additions, deletions, and changes to the ORB servers.

Copying or moving a server

You may want to move or copy a server to another host system on the system. To avoid re-entering all the configuration values, you can make a copy of a server through Avaya IC Manager, rename the new server, and move it to the new host machine.

To make a copy of a server

1. In Avaya IC Manager, click the **Server** tab.
2. In the right pane, right-click the server that you want to copy and select **Copy**.

   Avaya IC Manager displays the **Server Editor**. The server is given a new port number (one higher than the highest port number on this system) and a new name (the old name with _Copy appended). Avaya recommends that you change the default name. All other configuration parameters are copied from the old server to the new one.
3. Click **Apply** or **OK** to add the server to the Avaya IC Manager window.

Deleting servers

To delete a server in Avaya IC Manager:

1. In Avaya IC Manager, click the **Server** tab.

2. In the right pane, right-click the server that you want to delete and click **Delete**.

CAUTION:
Use this feature with caution. Deleting a server that is being used by a client or other process may adversely affect the system and result in data loss.

Synchronizing multiple Directory servers

The Directory server is responsible for maintaining a list of all the servers in Avaya IC. When multiple Directory servers are installed over a wide area network (WAN), they share one common directory. One Directory server must be responsible for synchronizing the directories and ensuring that changes made by one Directory server are reflected throughout the network. This Directory server is called the parent or master. It is identified by an asterisk (*) in Avaya IC Manager.

If there is only one Directory server in Avaya IC, it is automatically assigned parent status.

Note:
Avaya recommends that the parent Directory server be physically located at the site where the majority of changes to the directory occur.

When adding a new Directory server

1. Using Avaya IC Manager, create the new Directory server. Ensure that the host system of this new server is running an ORB server. (For details, see Creating a server on page 74.)
2. Backup the original Directory server, as described on Backing up and restoring server configuration information on page 38.
3. Copy the backup directory file from the host system of the first Directory server to the host system of the new Directory server.
4. Using Avaya IC Manager, start the new Directory server. It re-synchronizes with the parent Directory server before it starts, and that may take a few moments. (For details, see Starting or stopping a server on page 78.)

To change the parent Directory server:

1. In Avaya IC Manager, click the **Server** tab.
2. In the right pane, select the Directory server to be assigned as the parent.
3. Double-click the server.

   Avaya IC Manager displays the **Edit Server** window.
4. Click the **Directory** tab to display the configuration options.
5. Select the **Parent** check box.

   The check mark indicates that the server is now the parent, and Avaya IC Manager automatically clears the check mark for the Directory server which was previously parent.

Note:
You must select a new server to change the existing parent Directory server.

The timing of directory updates is affected by the update lag settings on this tab as well as by the **Auto Commit** option on the **Server** menu:

- Increasing the first update lag causes a delay before updates are sent from this directory. When importing information to the directory, Avaya recommends using a setting between 10 and 90 seconds. During normal operation, set the update lag value to 0 or 1.
- Increasing the succeeding update lag causes a delay before the parent sends an update to each succeeding child. When importing information from a list to the directory, Avaya recommends using a setting of 5 seconds.

Configuring Web Management servers

Avaya Web Management is the part of Avaya IC that provides real-time communication via web and email for personalized customer support. It lets companies offer their customers almost immediate access to a contact center agent, or customer service representative, from the company's Website.

Customers click a button on the site to send email or request a chat session (a real-time text conference). Web Management routes the request to an agent who can quickly interact with the customer.

Note:
Emails are not necessarily delivered in the First in - First out order.

Shared browsing

During the chat session, agents can also collaborate with a customer using shared browsing. This optional feature of Web Management lets an agent:

- Synchronize their browser with customer so that they both can view the same information
- Send information (such as a URL) directly to the customer's browser

- Assist a customer with filling an online form using the Shared Browsing feature (although the agent cannot submit the form for the customer). For more information, see Setting up Shared Browsing on page 340.

Frequently Asked Question database

Customers can also use the Web Self-Service feature to search a Frequently Asked Question (FAQ) database on the company's site, which provides them with a self-help source of information. For more information, see Setting up the Web Self-Service feature on page 320.

If you are using Avaya Content Analyzer, Web Management can auto-respond to some customer emails to let them know that their messages have been received by the system. In addition, it can attempt to answer the more common questions by comparing keywords in the customer's message to the FAQ database. (For details, see Chapter 7: Using Content Analyzer for automated email processing on page 170.)

Web Management interfaces

Web Management provides different interfaces for different users:

- Avaya Agent

  Contact center supervisors and agents use the Avaya Agent to interact with customers via Email and Web sessions. For details about this application, see the *Avaya Agent User's Guide.*

- Avaya IC Manager

  System administrators use the Avaya IC Manager to configure and manage the Web Management servers and environment.

  This chapter discusses about managing servers. For more information, see Understanding Web Management servers.

- Customer client

  Customers accessing the website of your company use a customer client, which consists of web pages designed to work with Avaya Agent. From these pages, the customers of your company and potential customers can send an email, request a chat session or use your self help library.

  The Customer HTML Chat Client is available with Avaya Web Management (Web Management). The Customer HTML Chat Client provides functionality in an HTML format that does not require contact center customers to install the Sun JVM on their systems before they can chat with an agent.

  For more information, see Chapter 14: Tenant websites on page 326 and Chapter 11: Avaya IC Customer HTML Chat Client on page 252.

For information about installing the Avaya Agent Web Client application server, see *IC Installation and Configuration*.

This section contains the following topics:

- Understanding Web Management servers on page 83
- WebACD server statistics on page 83

- Working with WebACD tasks on page 84
- Viewing ICM service status on page 86
- Viewing historical chat logs on page 87

Understanding Web Management servers

Web Management uses the following servers:

- Data server
- Communication Hub (ComHub) server
- Web Agent Automatic Contact Distributor (WACD or WebACD) server
- Attribute server
- Paging server
- Internet Call Manager (ICM) service

  For details on setting the properties for ICM service, see Chapter 6: Additional configuration options on page 136. For information on installing this service, see IC Installation and Configuration.

For details about these servers, see Managing servers on page 62.

In addition, two Web Management filters are installed on the web server:

- The WebAdmin plugin instructs the web server on how to handle certain types of administrative requests from a web browser, allowing dynamic generation of HTML content for administering the WebACD server.
- The dwsensor plugin is used for recording DataWakes. The plugin sends information about a users path through a Web site to the Attribute server for recording in the data store.

WebACD server statistics

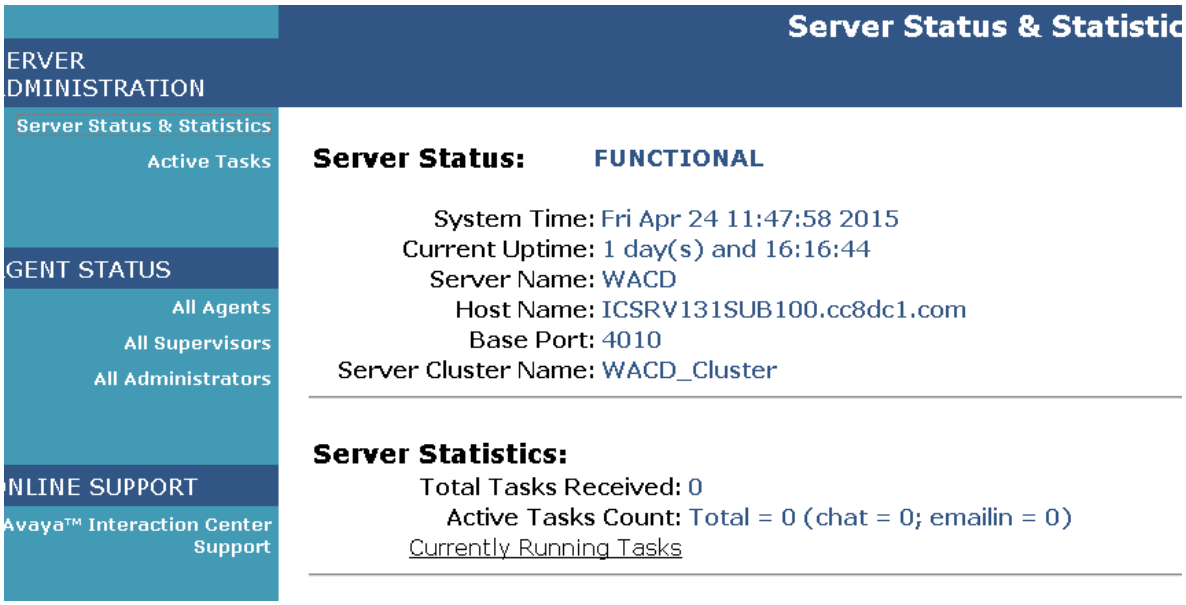
The Interaction Center WebACD Server page in the IC Web Management Administration Tool lets you to view WebACD server status, cancel or re-queue active email tasks, cancel chat tasks, or view agent status for the Web and email channel.

To access the WebACD server page:

1. In Avaya IC Manager, select **Services** > **WebACD**.

2. In the left pane, select **Server Status & Statistics** in the **Server Administration** section.

   The IC Web Management Administration Tool displays the **Server Status & Statistics** page that shows the top level WebACD information, such as server uptime, the number of chat and email tasks received since the last restart, and the number of active tasks.



To view the active tasks, select **Currently Running Tasks** at the bottom of the page. For more information, see Working with WebACD tasks

Working with WebACD tasks

To view information about currently running tasks:

1. In Avaya IC Manager, select **Services** > **WebACD**.
2. In the left pane, select **Active Tasks** in the **Server Administration** section.

   The IC Web Management Administration Tool displays the **Task List** page, which shows task information, such as the task ID, priority, task type, question asked (or email subject line), and agent and routing information.

Using the drop-down lists at the bottom of the **Task List** page, you can:

- Filter the task list by agent name, task type (queue), priority, and conversation (media) type.
- Sort the tasks from oldest to newest or vice versa

To change the number of tasks displayed per page, enter the maximum number of tasks you want to see in the **Max Tasks** field and select **Restart**. To view the next page of tasks, click **Next**.

To refresh the list and return to the first task, click **Restart**.

WebACD task priority

The order in which a task is entered into the WAITING_FOR_AGENT_ASSIGNMENT state for an individual Team Queue is known as the order of priority. The higher priority tasks are routed first.

The different queues in which a task moves back and forth are:

- **Service Queue**: The queue used by scheduler to run task state machine based on time stamp associated with a task.
- **Team Queue**: The queue associated with a workgroup. There is an individual queue for each workgroup. The system routes tasks to this queue and sorts the tasks based on their priority. When an agent in a workgroup is available, the top most task in the queue is removed and is assigned to the agent.

WACD supports the following priority levels for the tasks:

- LOW
- NORMAL
- HIGH
- URGENT
- SYSTEM

The tasks that are initially created are assigned to the available agents in the first-in-first-out (FIFO) order.

When agent transfers an email or chat to another agent, WASCD sets the priority of that task to SYSTEM This is because the task has already spent time in the queue before being assigned to the agent who initiated the transfer. Since the task has the System priority level now, it is placed above all other priority tasks. The task state in this case becomes WAITING_FOR_AGENT_ASSIGNMENT.

.

Routing On No Answer (RONA) is a special case in which FIFO order can alter. Let's understand this using an example. There are three tasks, task1, task 2, and task3 with NORMAL priority. For the first time, WACD assigns the WAITING_FOR_AGENT_ASSIGNMENT state to the tasks in the task1, task2, and task3 order. Now agent1 and agent2 are available and task1 and task2 are routed to the available agents. However, the agent does not accept the task and RONA happens in the order of task2 and task1. Now task2 and task1 have SYSTEM priority, so the order of Queue is task2, task1, and task3. If agent1 is available, then task2 is routed to to agent1 ahead of other tasks.

So the last task to which RONA happened is at the bottom of the SYSTEM priority task in a particular team queue.

It is important to note that the contacts in queue with particular priority are always delivered in order. Hence contacts t1, t2, t3 with System priority are always delivered in that order, let us assume there is already delivered task t4 and RONA happens for task t4 then it will be queued with SYSTEM priority and hence it will be placed after t3.

Reassigning email tasks

If an email task is active, inactive, or deferred, you can tell Avaya IC to send the task back to the qualification workflow so that it can be reassigned to a different agent. That way, if an agent cannot finish the emails in their queue, the administrator can reassign those emails without logging to the agent's logon ID.

To remove an email task from the queue of an agent:

1. In the task list, select the check box in the leftmost column for each active, inactive, or deferred email task that you want to reassign.
2. Select **RequeueTask(s)**.

Web Management removes the email task from the queue of an agent and sends it back to the qualification workflow so that it can be reassigned to a new agent.

Cancelling tasks

To cancel a currently running task:

1. In the task list table, select the check box in the leftmost column for each task that you want to cancel.
2. Click the **Resolve Status** field and select the appropriate status to cancel the selected task.

   The **Resolve Status** field displays the status messages that you configure in Email Template Administration. For more information on creating the status messages, see Creating statuses on page 98.
3. Click **Cancel Task**.

Note:
Email tasks will be recorded as abandoned if the tasks are cancelled in this manner, even if they have not been accepted by an agent.

Viewing ICM service status

An information alarm is displayed in Avaya IC Manager when the ICM server is stopped or started.

Note:
If a user uses the Windows Restart Service feature to restart the ICM service and if the service starts immediately, the Attribute server might not connect to the ICM service. In such a scenario, restart the Attribute server or stop the ICM service and wait for 25 to 30 seconds and restart the service.

Viewing historical chat logs

To view the chat log associated with a particular task:

1. In Avaya IC Manager, select **Services** > **Web Response Unit**.
2. In the left pane, select **Web Self-Service Console**.
3. Select **View Transcripts**.
4. Select a task ID from the drop-down list at the top of the page and click **Submit Query**.

Enabling the SSL security for the Directory server

IC Clients uses a secure channel to log in to the VESP framework. The Directory Server now listens the SSL login requests on a different port, apart from the VESP port. Only the login requests are routed to the SSL port. All the other requests are routed to the existing VESP port.

To enable the SSL security for the Directory server:

1. In IC Manager, on the **Servers** tab, right-click the **Directory** server for which you want to enable the SSL security and select **Edit**.
2. In the Directory server properties dialog box, click the **Directory** tab.
3. Right click on the Directory page and select the **Show Advanced Properties** check box.
4. Verify that the following fields contain the correct values for the SSL configuration.
   - Certificate File
   - Key File
   - SSL Socket Port
   - Update LDAP Config on Generic Update
   - DHParam File

   For more information about the SSL configuration fields, see Directory tab on page 454.
5. Keep the default values in the **Certificate File**, **Key File**, and **HTTPS Port** fields.

   Note:
   In the **Key File** field, if the specified key file is encrypted with Passphrase, you must create a new entry for the Directory server in the **Private Key PassPhrase** configuration. Do not create an entry if the key file is not Passphrase protected.

   For more information about PassPhrase for the Directory server, see Private Key PassPhrase table folder on page 144.
6. Click **Apply**.

7. Stop the Directory server and again start the Directory server.

Configuring the passphrase information

You can passphrase protect the SSL certificate private key file for the Directory server. You must configure this passphrase protection on the Configuration tab of IC Manager.

After configuring the SSL certificate private key file passphrase information for the Directory Server, IC Manager stores that information in the `ds.ffd` file in an encrypted format.

To configure the passphrase information in IC:

1. In IC Manager, Click the **Configuration** tab.
2. In the left pane, select **Private Key PassPhrase** > **Directory Server**.
3. On the toolbar, click the **New** button.
4. Click the **Directory** Server drop-down list and select the name of the Directory server for which you want to configure the passphrase.
5. Click the button next to the **Password Phrase** field.
6. In the setPassword dialog box, enter the password in the **Password** and **Confirm Password** fields.
7. Click **Ok**.
8. On the Configuration page, click **Ok**.

Reconfiguring the database and generating the Windows application

There are changes to the database schema for the IC-LDAP integration. These changes are available through ADL files present in the `IC_INSTALL_DIR\design` directory.

To update the database with new records for IC-LDAP integration:

1. Open DB Designer.
2. In DB Designer application, open the `repository.adl` file.

   For more information, see *IC Database Designer Application Reference*.
3. Reconfigure the database, and regenerate the windows application.
4. Repeat the Step 2 and Step 3 for the `ccq.adl` file.

Enabling the SSL security for the HTTPConnector server

After enabling the SSL security for the HTTPConnector server, you must deploy the root / CA certificate in Orchestration Designer / Dialog Designer.

For more information deploying the certificate in Orchestration Designer / Dialog Designer, see the documentation provided with Orchestration Designer / Dialog Designer.

To enable the SSL security for the HTTPConnector server:

1. In IC Manager, on the **Servers** tab, right-click the **HTTPConnector** server for which you want to enable the SSL security and select **Edit**.
2. In the HTTPConnector server properties dialog box, click the **HTTPConnector** tab.
3. Select the **Enable SSL** check box.

   By Default, the **Enable SSL** check box is not selected, so the HTTPConnector server works in a conventional TCP mode. After you select the **Enable SSL** check box, IC Manager displays the following fields with the default configuration for the HTTPConnector server to work in the SSL mode:

   - Certificate File
   - Key File
   - HTTPS Port

   For more information about the SSL configuration fields, see HTTPConnector tab on page 475.
4. Keep the default values in the **Certificate File**, **Key File**, and **HTTPS Port** fields.

   You must keep the certificate file, and key file in the `IC_INSTALL_DIR\etc\` directory.

   If you want to generate the server certificate, use the Fully Qualified Domain Name (FQDN) of the server hosting the HTTPConnector server as the Common Name (CM). Also, add the FQDN and IP mapping in the host file of the server hosting the Orchestration Designer / Dialog Designer application and use the same FQDN as the address of HTTP Server on the Orchestration / Dialog Designer Admin page.

   Note:
   In the **Key File** field, if the specified key file is encrypted with Passphrase, you must create a new entry for the HTTPConnector server in the **Private Key PassPhrase** configuration. Do not create an entry if the key file is not Passphrase protected.

   For more information about PassPhrase for the HTTPConnector server, see Private Key PassPhrase table folder on page 144.
5. Click **Apply**.
6. Stop the HTTPConnector server and again start the HTTPConnector server.

Chapter 5: Email services

Avaya IC Manager provides support for the following email services:

- Email templates
- Avoiding email autoresponse loops
- Email accounts
- Email filters
- Email approval process

You can configure these services and filters using the Avaya IC Manager.

This section contains the following topics:

- Email template administration on page 90
- Avoiding an email auto response loop on page 106
- Formatting an HTML email message on page 108
- Email accounts on page 111
- Email approval process on page 129

Email template administration

Message templates are *form letter* responses that Email Management uses to automatically answer email, and to provide additional information on agent replies to user email. Templates can also be used to add a header or footer to each outgoing message, or to automatically inform users about the status of their messages.

Message templates are used in several places by Email Management:

- To acknowledge receipt of an incoming message, and provide a tracking number
- To apply header and footer text automatically to every outgoing message
- To send *rejection* messages for a particular business case using the "resolve with status" feature of Avaya IC. Examples of business cases using the *Rejection* template are mentioned later in this section.
- To append f*orm letter* text to replies sent by agents

Here are some ways to make the most of Email Management's templates:

- Customize your *Message Response* templates for each queue. Include answers to frequently asked questions, pointers to your web site, and contact information.
- Use the Header and Footer information to add text to the beginning and end of every message sent by an agent. Be creative and promote your products and services on every outgoing message. Remember, each queue can have its own set of headers and footers.
- Use Status templates to keep customers informed about the progress of their inquiries. Some support messages, for instance, require an agent to research the answer to a customer's question. Agents apply a status through a web form in Email Management, that automatically sends a *form letter* to the customer on every outgoing message advising them of the reason for the delay. Your customers know they're being looked after, and haven't been forgotten.
- Use the *Rejection* template to promote a prepaid *members-only* email support subscription service or other *by-invitation* messaging service.

Managing templates and statuses

In IC 7.3.2 FP, the folders can be mapped to workgroups. This ensures the following:

- Restrict the template and status downloading at the agent's side.
- Increase the performance improvement as less number of templates is downloaded at the agent side.
- Ensure that only the relevant templates are accessible by the agent.

Use the folder disabling option to restrict the contents of the folder from being shown at the agent side. This is applicable from IC 7.3.2 FP onwards.

The administrator can access and modify all the folders, templates, and statuses. The supervisor can access all the folders and their contents but can only modify the folders and their contents which are mapped to the workgroup of the supervisor.

The templates visible to the agent depend on the folder-workgroup mapping of the agent's workgroup and the template download properties set in IC Manager. See the Agent Properties section. However, the templates and statuses configured at root level would be visible to all the agents irrespective of the property value and workgroup mapping.

Inheriting workgroup mapping

The subfolders can inherit the workgroup mapping from the parent folder. In this case, all the workgroups mapped to the parent folder will also be mapped to the subfolder. Out of the box, all the workgroups present in the system are mapped to the root folder and the inheritance is ON.

Note:

In RL Manager, if you want to map the child workgroups to a folder, you must explicitly map all child workgroups to the required folder. By default, the child workgroups from the parent workgroup are not mapped to the folder when you map the parent workgroup to a folder.

Best practices:

Place all the templates and statuses common for all at the root level or put them in a subfolder of the root folder with the inheritance ON.

If a particular folder must be viewed only by agents of a particular workgroup, disable the inheritance for the folder and directly map the particular workgroup to the folder.

Note:

The time required to complete the Refresh Email Templates operation from the JavaAppBridge server in IC Manager varies according to the number of templates that are configured in the system. For example, if there are more than thousand templates, the operation might take five to ten minutes depending upon the size of the templates.

If an agent logs in before the Refresh Email Templates operation is complete, then the templates are not available to the agent. The agent must close and open the resource window again to view the templates after the caching operations is complete. Run the Refresh Email Templates operation during non-peak hours to save time.

In IC Manager, you can access the **Email Template Administrator**, by selecting **Services** > **Mail Template Administration**. You need to enter your Avaya IC Manager logon ID and password.

This section contains the following topics:

- Email templates with attachments on page 93
- Organizing the content on page 93
- Creating templates on page 93
- Modifying a template on page 94
- Refreshing email templates on page 95
- Deleting email templates on page 95
- Multi-language support for email templates on page 96
- Creating folders and sub-folders on page 96
- Modifying a folder on page 97
- Creating statuses on page 98
- Modifying a status on page 99
- Setting the Answered status to a message on page 99
- Applying an autoresponse template to a status on page 100
- Associating resolve statuses with email templates on page 101
- Associating the template with a status on page 101
- Template macros on page 102
- File attachments on page 104
- Sample message templates on page 105

Email templates with attachments

Email templates with attachments are primarily used when using the templates as part of the IC Email auto-response functions. Avaya Agent only supports use of the text part of the template. The template in the agent resources does not display any associated attachments.

If resources have to be used where attachments need to be specified, email resources can be created. These resources are separate from email template resources. Email resources allow the agent to specify the to, cc, bcc, subject, body and attachments when creating the attachment.

These should be created and used if the agent wants to use resources with attachments. Care should be taken to ensure that the attachments specified are accessible from the agent's system. This is especially important when the email resource has been defined as part of the global resources hierarchy.

Organizing the content

The **Template / Status** tab allows you to organize templates and statuses in folders, thus creating a tree structure that groups items in a logical way.

You can organize templates and statuses in folders by topic, or by department, or according to any other logically consistent pattern. The more care you take to organize your templates in this window, the more productively your agents can use these templates when responding to customer messages.

You organize your templates and statuses by creating and naming folders, then moving the templates and statuses into folders. You can also create sub-folders in any number of levels, however you should take care not to create a structure that is more complex than it needs to be, otherwise you and your agents may have to spend more time than necessary searching for items in the list.

Tip:
Items in this list are sorted alphabetically. You may want certain items, for instance **resolve** statuses that do not send an autoresponse, to always appear at the beginning of the list so your agents can locate them easily. To do this, precede the item name with a punctuation character such as an exclamation point (!) or asterisk (*) that sorts ahead of the alphabetic characters.

Creating templates

Templates in Email Management can be

- Associated with queues to send automated reply messages, headers and footers. Templates can also be sent automatically in response to certain system events, such as autoresponder loop detection and blank message detection.

- Associated with agent-selectable statuses to resolve messages and send a prepared reply to a frequently asked question (FAQ).
- Sent as an automated response based on the rules defined in a workflow. This is similar to the FAQ feature, but the workflow can do additional processing before it determines which template to send.

To create a template:

1. In Avaya IC Manager, select **Services** > **Email Template Administration** and click **Content**.
2. Browse the list of folders and templates until you find the template you wish to modify. Select **New**, and then select **New Template**.
3. On the **General** tab, enter the name of the template.
4. In the **Language** field, click the language in which you want to create the email template.
5. (Optional) Select **Use original message subject** if you want autoresponse to use the subject of the incoming email

   You can ignore the **Use original message subject** check box if you want a new subject in the **Subject** field.
6. On the **Message** tab, enter a message in the **Message** window or select **Import** to import a valid file type (the valid file type depends on what applications are installed on your system).
7. You can attach one or more files to the template, which can be sent to a user when a message is resolved to the status corresponding with this template. On the **Attachments** tab, click **Add** to browse for a file to attach to this template.
8. Click **OK** when you finish creating the template.

Modifying a template

To edit a template:

1. In Avaya IC Manager, select **Services** > **Email Template Administration** and click **Content**.
2. Browse the list of folders and templates until you find the template you wish to modify, and select **Properties**.
3. Click the **Message** tab to edit the template text. The **Editing** window on the **Message** tab uses standard editing keys to cut, copy, and paste text.

   Use Template Macros to insert variable information such as date, time, and queue name in your templates. Email Management replaces the macros with the corresponding information when it sends your message template to a user. Note that template macros are translated only in automatic responses and status responses. Macros are *not* translated when they are used in items that are copied and pasted from the Response Library.
4. Click **Import** to import a text file stored on disk.
5. Click **Ok** when you finish editing your template, or click **Cancel** to discard your changes.

Refreshing email templates

In Avaya IC, the Java Application Bridge caches the email templates on a system where Java Application Bridge is running. However, if the supervisor updates the email templates, the cache needs to be refreshed for the updated templates.

In Avaya IC Manager, you can use the **Refresh Email Template** button to refresh the email templates in the cache. The time required to complete the **Refresh Email Templates** operation performed from Java Application Bridge varies depending on the number of templates that you configured in the Avaya IC system. For more than 1000 email templates, the system can take 5 to 10 minutes to complete the **Refresh Email Templates** operation depending upon the size of the templates.

While the system is performing the **Refresh Email Templates** operation, agents cannot use the email templates. If an agent logs in to Avaya Agent Web Client before the **Refresh Email Templates** operation is complete, the agent cannot view the email templates in the Web Client interface. Once the **Refresh Email Templates** operation is complete, agent can close the resource window and open the window again to view the templates.

Avaya recommends performing the **Refresh Email Templates** operation during the non-business hours.

To refresh email templates:

1. In IC Manager, on the **Server** tab, right-click the Java Application Bridge server name and select **Edit**.
2. Click the **JavaAppBridge** tab.
3. Click the button next to **Refresh Email Templates**.

   The system displays a message dialog box indicating that the email templates are successfully refreshed.
4. Click **Ok**.

Deleting email templates

You can delete email templates that you no longer require.

To delete email templates:

1. Locate and select an email template that you want to remove.
2. Click **Delete**.
3. Click **Ok**.

If you delete a folder, all the items in the folder are deleted as well.

Multi-language support for email templates

In RL Manager, you can create email templates that support multiple languages. You can use these email templates for sending acknowledgments. Usually, you need to select a language when you create or edit an email template. However, this restricts that email template to a single selected language. So, if an email contains characters from a language other than the English language, the email message displays those characters either as boxes or arrows when the customer receives that email. Therefore, to create email templates consisting of more than one language, a new **Multi-Language** option is added to the **Language** field on the create or edit email template page.

Note:

When you use the Multi-Language option in an email template, the time format is set to 24-hour time format.

Multi-Language support templates are currently not supported to use as Header or Footer templates.

Creating folders and sub-folders

Folders can contain statuses, templates, or sub-folders. Each folder must have a unique name.

To create a folder

1. From Avaya IC Manager, select **Services** > **Email Template Administration**.

   Avaya IC Manager displays the **Email Template Administrator**.

   Note:

   If the **Email Template Administrator** does not open, Ensure that the `EmailLoginServer` property is correctly specified in the **System/Configuration** section of the **Group Manager** for the **IC** system entity. For more information, see System/Configuration property descriptions on page 644.

2. Click **New**.
3. Click **New folder**.
4. Enter the name of the folder in the **Name** field.
5. Check the **Disable this folder and its contents** check box only if you do not want this folder to be displayed to the agents.
6. Go to the **Advanced** tab, update the workgroup mapping for the folder.
   1. Check the **Inherit workgroups mapped to the parent folder** check box if required. This populates the workgroups mapped to parent folder inside the **Inherited** section of the mapped workgroup list.
   2. To directly map workgroups to the folder, select the workgroup from the available workgroup list.

   3. Click **Add**.
7. Click **OK**.

Note:
You cannot remove an inherited workgroup by clicking the Remove button.

Steps 5 and 6 are applicable on to IC 7.3.2 FP onwards.

Modifying a folder

To modify a folder

1. From Avaya IC Manager, select **Services** > **Email Template Administration**.

   Avaya IC Manager displays the **Email Template Administrator**.
2. Click **Content**.
3. Browse the list of folders and templates until you find the folder you wish to modify, then select **Properties** to pop up the **Folder Properties** property sheet.
4. Make any necessary changes.
5. Click **OK**.

Note:
While changing the folder name from two or more threads at the same time, it is possible that the changes are not reflected in the tree until manual refresh.

Creating statuses

In certain circumstances, an agent may need to resolve a message without sending a response to the customer. (For example, when an issue has been resolved and requires no further action.)

To create a new status:

1. In Avaya IC Manager, select **Services** > **Mail Template Administration**.
2. If prompted, log in to the **Email Template Administrator** using login ID and password for Avaya IC Manager.
3. If you have created multiple folders under the **Content** list, select a folder where you want to create a new status. Otherwise, select the **Content** node in the tree.
4. Click **New**.
5. Click **New Status**. The **Email Template Administrator** displays the **New Status Properties** dialog box.
6. Enter the name of the status in the **Name** field. Avaya Agent displays this status name in the list of available statuses for agents. Do not include an underscore (_) in the status name unless you want to associate a language code with this status.

   If you associate a language code with a status, when an agent using Avaya Agent selects the **Filter by Language** option, they will only see those statuses (and their associated status templates) that are associated with the selected language.

   Important:
   The **Filter by Language** option is available only with Avaya Agent desktop. This option is not available with Avaya Agent Web Client.

   To associate a status with a language, append an underscore and one of the following language codes to the status name. When the agent views the list of statuses, Avaya Agent removes the underscore and the language code from the status name. Therefore, if you want to make it clear that a given status is associated with a given language, you should add your own language identifier that is not preceded by an underscore.

Language	Code
Chinese, Simplified	zh
Chinese, Traditional	zh_TW
English	en
French	fr
German	de
Italian	it

Language	Code
Japanese	ja
Korean	ko
Portuguese	pt
Spanish	es
Thai	th

7. Select from the following options:
   - **Messages set to this status should be treated as answered**. If the status indicates a resolution of the issue that requires no further action by the agent.
   - **Send template for this status**. To send an auto-response message to the user when an agent assigns this status to a message. Select a template to send.
8. Click **OK** to close the **Status Properties** dialog and add the new status.

Repeat the procedure for each status that you want to add.

Status descriptions are sorted alphabetically in the **Content** list window. To edit or view the settings for a status, select the status name from the list and select **Properties**.

To permanently remove (delete) a status from the list, select the status name from the list then select **Delete**. Confirm the deletion at the prompt.

Modifying a status

To edit a status:

1. In Avaya IC Manager, select **Services** > **Email Template Administration**.
2. Click **Content**.
3. Browse the list of folders and templates until you find the status you wish to modify. Select **Properties** to pop up the **Status Properties** property sheet.
4. Make the necessary changes.
5. Click **OK**.

Setting the Answered status to a message

Certain message statuses can be designated as *answered*. This information is recorded in Email Management's statistical databases, and can be used to provide information on the total number of messages answered for a specified reporting period.

To define Answered status:

1. In Avaya IC Manager, select **Services** > **Email Template Administration.**
2. Click **Content**.
3. Browse the list of folders and templates until you find the status you wish to modify. Select **Properties** to pop up the **Status Properties** property sheet.
4. To turn on Answered status, select the **Messages set to this status should be treated as answered** check box.
5. When you finish filling in status information, click **OK**.

Applying an autoresponse template to a status

Agents can manually assign a **status** to an incoming message, to indicate for instance that the issue is being researched, or that it was forwarded to a supervisor or another agent for action. You can automatically send a message to a user each time an agent changes the message status.

To apply a template to a change of status:

1. Create a template.

   For more information, see Creating templates on page 93.
2. Associate the template with an autoresponse status:
   a. Click **Content**.
   b. Click **New** to open the **New Status** dialog box.
   c. On the **Status Properties** dialog box, fill in the name of the status to assign. This text will appear in the list of statuses in the Avaya Agent **Resolve Message** dialog box.
   d. If the status indicates a resolution of the issue that requires no further action by the agent, select the **Messages set to this status should be treated as answered** check box.
   e. To send an auto-response message to the user when an agent assigns this status to a message, select the **Send template for this status** check box. Select a template to send.

Note:

When the primary IC email server fails and the secondary IC email server becomes active, the email channel status changes to **Impaired** for the agents logged in using AAWC or SDK. In AAWC, a cross sign appears on the email channel when the status is **Impaired** and the sign disappears when the email channel is available. In SDK, the UI representation may vary depending on the implementation to represent the channel availability information.

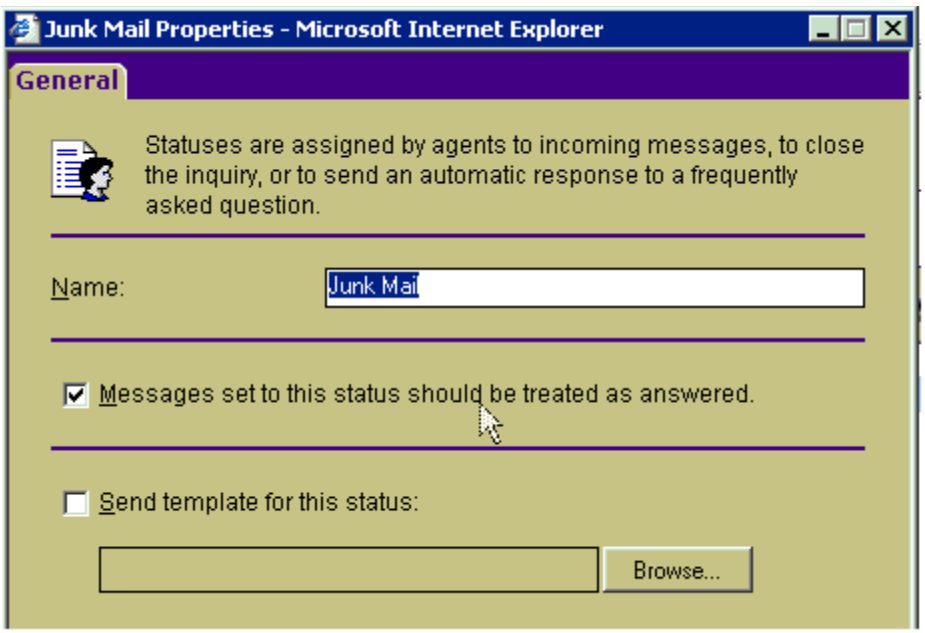
If the email channel status is **Impaired**, the agent cannot receive new incoming emails or send emails. However, the agent can compose new emails and read the old emails. After two or three minutes, the email channel status changes to **OK** automatically. The agent can continue working normally without logging off and logging again.

Associating resolve statuses with email templates

The **Release with Reason** sub-menu in Avaya Agent Web Client consists of folders, sub-folders, and a set of resolve statuses that have been created in Avaya IC Manager with the **Messages set to this status should be treated as answered** option set. The sub-menu becomes visible when there are resolve statuses configured. If resolve statuses are configured, the sub-menu remains visible until the wrap-up phase is entered.

Resolve statuses have the option of being associated with an email template. When you select the resolve status, the contact is released and the associated email template is sent to the customer.

The following window is displayed in Avaya IC Manager when creating resolve statuses. The **Name** field for each configured status is used as the display name in the release reasons sub-menu. Email templates are built elsewhere in Avaya IC Manager, but they can be associated with a resolve status in this window.



Associating the template with a status

You can automatically associate a status with a template. When your agents resolve a message with this status, the template text will be sent to the customer as a reply.

To do so, select the **Create associated status** to create a status using this template check box.

Template macros

Using Template macros you can personalize a form letter response to a user with variable information such as date and time, queue name, and tracking number.

When Email Management sends a template message to a user, it scans the text for macros it recognizes (text surrounded by the % character), and fills in the text referenced by the macro. The result is a message that can include variable data such as time, message status, queue name and tracking number.

Email Management recognizes and translates the following template macros:

Macro	Translation
%AGENTNAME%	The responding agent login ID (used only in "Reply" template).
%DATE%	Current date in system date format.
%MESSAGESTATUS%	The message status description.
%POOLFOOTER%	The text from the "footer template" specified for this queue.
%POOLHEADER%	The text from the "header template" specified for this queue.
%POOLNAME%	The queue name.
%QUOTEMESSAGE%	The text of the original message.
%RECIPIENTNAME%	The message recipient email address.
%SUBJECT%	The subject line of the message.
%TEMPLATENAME%	The name of the template, as configured in eContact Web Manager.

Macro	Translation
%TIME%	Current time in system time format. Avaya IC supports the 24 hour time format in the email template for the countries using the following languages: • Traditional Chinese • Simplified Chinese • Korean • Japanese • Thai • English • German • French • Italian • Spanish • Portuguese • Russian **Note:** You must restart the Avaya IC servers if you change the time format. While converting time from 12 hour format to 24 hour format and from 24 hour format to 12 hour format, the system does not consider Daylight Saving Time (DST). This feature is supported on all platforms supported by Avaya IC (Windows, Solaris, and AIX). To set the 12 hour or 24 hour format for any particular locale on AIX and Solaris: 1. Correctly add the `d_t_fmt` and `t_fmt` descriptors in the **LC_TIME** section of the locale source. **Note:** `d_t_fmt` and `t_fmt` are the operating system related descriptors. 2. Stop the Avaya IC servers on the system. 3. Run the following command: `export LC_TIME=<locale_name>` 4. Verify the time format using the following commands: date date +%X 5. Start the Avaya IC servers on the system.

Macro	Translation
%TRACKINGNUMBER%	Tracking number.

For an example of a message template that uses macros to fill in the recipient's name, the queue name, the message date and the message time, see Example message template on page 105.

Tips for creating macros

- The Agentname macro inserts the login ID of the agent responding to a message from a user. Email Management does not provide this information in replies. However, it directs users to reply to the message queue, which allows Email Management to maintain a continuous exchange of messages.

  This macro is valid in "Reply" templates, headers, and footers. It should not be used in automatic responses to the original message from a sender, because at that point Email Management has assigned only a message queue, not an agent, to deal with the message from a user.

- When an agent assigns a Status to a message, Email Management can optionally send an autoresponse message to the user. You can use the Messagestatus macro to insert the *status* text (defined in **Email Template Administrator**) in the autoresponse template associated with the status.

  This is useful when you use the same *generic* template for more than one *status* autoresponse messages. The Messagestatus macro can be used here to briefly explain the reason for the change of status

- Poolname is the name of the queue associated with the mail account of a user. These queues are not the same queues used in routing of email tasks.

- Date and Time macros are filled in with the current system date and time These macros are mainly useful to indicate the date and time of an automated response to the message from a user.

- The Trackingnumber macro inserts the unique tracking number assigned by Email Management to the original message from a user. The tracking number is always included in the subject line of the message. However if you wish, you can also refer to it in the text of an autoresponse message.

File attachments

Email Management allows you to attach one or more files to send with a template.

To attach a file to a template

1. In Avaya IC Manager, select **Services** > **Email Template Administration** and click **Content**.
2. Browse the list of folders and templates until you find the template you wish to modify, then select **Properties**.
3. Click the **Attachments** tab. Click **Add** to select a file to attach to the template.

Note:
The ability to receive and save attachments depends on the capabilities of the recipient's email system. Although you can attach any number of files to a template, not all email programs can receive multiple attachments. The total size of the template plus its attachments may exceed the capacity of some email servers and email programs.

Sample message templates

The following sample templates illustrate how you can use variables to personalize an automatically-generated email message.

Example message template

```
Dear %recipientname%,

This is an automated response from %poolname%.

We received your message on %date% at %time%.

Our staff is available to respond to messages during regular business hours, excluding
holidays. Messages are normally answered within one business day.

You should be receiving a personal response by email from one of our staff shortly. In the
event you need to contact us regarding your original message, please refer to the tracking
number at the top of this message. This will help our staff locate and review your
correspondence with us.

Thanks once again for writing. You should hear from one of our staff shortly.
```

Example status template

```
Dear %recipientname%,

This is an automated response from %poolname%.

We received your reply on %date% at %time%.

Our staff is currently investigating the questions you asked in your message, and hope to have
an answer for you shortly.

In the event you need to contact us regarding your original message, please refer to the
tracking number at the top of this message. This will help our staff locate and review your
correspondence with us.

Thanks once again for writing. You should hear from one of our staff shortly.
```

Example autoresponse loop detection template

```
Because we have received 10 email messages from your email address within the last 24 hours,
we will not send any further automated response messages to you for the next 24 hours. Any
further mailings will be accepted, however confirmation will not be sent.
```

```
Thank you for your interest in Avaya Incorporated.
```

Example rejection template

```
Dear %recipientname%,

This is an automated response from %poolname%.

We regret that we were unable to deliver your message because the return address on your email
did not match the list of addresses recognized for this message pool.

Please check the configuration of your email program to confirm that the return address is the
same as the one registered to you in our customer files, then send your message again.

If you are not registered in our customer files, we invite you to contact us by telephone to
enroll in our support program.
```

Avoiding an email auto response loop

Many email users configure their email applications to automatically send a response every time an email message is delivered to the user's mailbox. For example, users can configure their email application to notify a sender that the user is on vacation or away from their desk for the day.

These automatic messages can create serious problems for programs such as Email Management if it is configured to respond automatically to all incoming messages. A situation can quickly develop where autoresponders at each end get into a never-ending dialog loop.

Email Management allows you to limit possible autoresponder loops by specifying a maximum number of messages that will be automatically responded to from any email address in a 24-hour period. If the number of messages from a user reaches that value, Email Management responds one more time with a template, then stops autoresponding to that user. Messages continue to be routed to agents, and agent replies are routed back to the customer. (For a sample template, see Example autoresponse loop detection template on page 105.)

Email loops can also be generated by workflow-initiated acknowledgements. To avoid this issue, make sure that the flow looks at `emailcount` field in the EDU. If the value of this field exceeds the required value, the flow should bypass the SmartAck block. For more information about the email workflows, see *Avaya IC Media Workflow Reference*.

Note:
For an email account, the information about the loop detection count is not synchronized between the primary Poller server and secondary Poller server. Therefore, when the primary Poller server fails, the secondary Poller server starts the loop detection count for that email account from one.

To turn on autoresponse loop detection:

1. In Avaya IC Manager, select **Services** > **Email Accounts**.

2. From the **Email Address** list, double-click the email address for which you want to turn ON the autoresponse loop detection.
3. Click the **Miscellaneous** tab.
4. Select the **Loop Detection** check box.
5. From the **Loop Detection Type** drop-down list, select the loop detection type.

   Loop detection type is based on "sender", "from address", "reply to address", or "both". You can select one of the following loop detection types:

Loop detection	Description
sender	Sender (first looks for Reply-To, if not set then looks for "from")
from	from address
replyto	reply to address
both	Both from address and reply to address

6. In the **Loop Detection Template** field, select the template used to send a final message to a customer after the message loop count is exceeded.
7. In the **Loop Detection Count** field, enter the maximum number of automated responses that you want the customer to receive in a 24-hour period.

   Email Management will not automatically respond to messages that exceed this count.
8. Click **Ok**.

Formatting email text

Avaya IC supports the following text formats for email messages and resources:

Plain text format: Plain text does not support any special formats in the body of an email message. Plain text does not support text formats or images.

HTML format: HTML supports special formats in the body of an email message. With HTML format, you can format the message text. For example, you can emphasize words with bold, italics, or colors. You can also view and insert images in an email message.

Note:
Web Agent does not support stationary or background images in emails. If a customer sends an email with stationary or a background image, Web Agent does not display the stationary background. Web Agent displays all other HTML formatting in the message, including any embedded images.

This section includes the following topics:

- Changing the message format on page 108
- Formatting an HTML email message on page 108

Changing the message format

The type of email message determines the message format:

- Replies and forwarded emails automatically use the same message format that Avaya Agent Web Client uses to display the original incoming email. For example, if Avaya Agent Web Client displays an incoming email in HTML format, your reply is also in HTML format.
- New outbound emails use the default format set in your preferences. To set the default format for all new outbound email messages, see *IC Administration Guide*.

If a reply or other outbound email is sent to an approver for quality assurance, the approver can change the format of the message. However, Avaya recommends that all email approvers set their email preferences to read incoming emails in HTML format. This setting ensures that Avaya Agent Web Client displays all emails that require approval in the format selected by the agent.

To change the message format, select one of the following options from the drop-down list on the HTML formatting toolbar:

- HTML
- Plain Text

Important:
If you change the format of an email message from HTML to Plain Text, you will lose all formatting, images, and other content that is not supported in plain text.

Formatting an HTML email message

You can format all HTML email messages that you create, including new outbound emails, replies to customers, and forwarded emails.

This section includes the following topics:

- Formatting message text on page 109
- Aligning text on page 109
- Changing the font colors on page 109
- Creating a bulleted or numbered list on page 110
- Inserting an image on page 110

Formatting message text

To format message text:

1. Select the text you want to format.
2. On the HTML formatting toolbar, click one of the following buttons.
   - Bold
   - Italic
   - Underline
   - Font
   - Font Size

Aligning text

To align text:

1. Select the text you want to align.
2. On the HTML formatting toolbar, click one of the following buttons.
   - Align Left
   - Center
   - Align Right

Changing the font colors

You can change the background color of selected text and the color of the text.

To change font color:

1. Select the text you want to format.
2. On the HTML formatting toolbar, click one of the following buttons:
   - Highlight Color to change the background color of the text.
   - Foreground Color to change the color of the text.
3. In the **Font Color** dialog box:
   a. Select the color you want to apply.
   b. Click **OK**.

Creating a bulleted or numbered list

To create a bulleted or numbered list:

1. Select the paragraphs that you want to include in a bulleted or numbered list.
2. On the HTML formatting toolbar, click one of the following buttons:
   - Bullets
   - Numbering

Inserting an image

You can insert any image that is located in a shared directory designated by your supervisor. Contact your supervisor if you cannot access this directory.

Note:
You can only insert images from directories specified by your supervisor. You must use file URL scheme for **Image URL** field:
file://<host>/<path>

Avaya recommends that you do not insert too many images in an email work item. If possible, use a link to an image on a Web server that the customer can access. The size of an email work item increases with each embedded image. Some customers may not be able to download a large email, especially an email that contains one large image or many smaller images.

To insert an image:

1. Place your cursor where you want to insert the image in the email message.
2. On the HTML formatting toolbar, click **Insert Image**.
3. In the **Insert Image** dialog box, in the **Image URL** field, type the location of the image.

   You can click Preview to view the Image Preview.
4. In the **Alternate text** field, provide the alternate text information about the image.
5. In the Layout section, you can specify the **Alignment** and **Border thickness** of the image.
6. In the Spacing section, you can specify the **Horizontal** and **Vertical** spacing of the image.
7. Click **OK**.

Email accounts

Email Management polls mailboxes on your POP3 (Post Office Protocol version 3) server or IMAP4 (Internet Message Access Protocol version 4) server for incoming messages. Some commonly used email accounts include "support", "sales" and "info".

When a message arrives at your site addressed to one of these email accounts, Email Management assigns the message to a queue where agents assigned to that queue can answer it.

Note:
In order for Email Management to receive email at these addresses, you must also create these email accounts and passwords on your POP3 and IMAP4 servers. Because the procedure for creating user names differs depending on what POP3 or IMAP4 server you are using, you should consult the documentation for your POP3 and IMAP4 software for instructions on how to add user names.

This section contains the following topics:

- Adding an email account on page 111
- Testing an email account on page 117
- Creating email filters in IC 7.3, 7.3.1, and 7.3.2 on page 123
- Creating email filters in IC Release 7.3.3 and later on page 124
- Deleting an email account on page 127
- Failure scenarios for incoming emails on page 128

Adding an email account

Before using Avaya IC Manager to add email accounts to Email Management, you must first verify that the mailbox you wish to add has been created on your POP3 and IMAP4 server. You should also make a note of the logon ID and password. Avaya IC Manager only links to an existing mailbox, it does *not* create the email account on your POP3 or IMAP4 server.

After you verify that the mailbox has been created and is working properly, you can add that mailbox to Email Management:

1. From the Avaya IC Manager, select **Services** > **Email Accounts**.

   The **Email Accounts** dialog box opens.
2. Click **New** to display the **New Email Account** property sheet.
3. Fill in the fields on the following tabs:
   - General tab
   - Outgoing Email Server

- Incoming Email Server
- Templates tab
- Filter tab
- Miscellaneous tab

Note:
After adding the first email account, whenever you create a new email account, IC Manager fills certain fields, such as Domain, Outgoing email server, Incoming email server, and Bounce email address with the information that you specified for the first email account.

General tab

The **General** tab contains general information about the email account that you want to configure.

In the **Display Name** field, enter the alias 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 that 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.

In the **Name** and **Domain** fields, you need to enter the mailbox name and domain exactly as they are configured in your POP3 or IMAP4 server. Note that Email Management can manage mailboxes in any number of domains so long as it has the necessary information to log onto the POP3 or IMAP4 server.

In the **Tenant** drop-down list, select the tenant that will be associated with this email account.

The return address is the address that appears in the “From” field in an email response sent to the customer from this account. Avaya IC Manager automatically fills in this address with `name@domain`. To use a different return address, select it from the **Return address** drop-down list.

You must select the poller cluster name from the **Owner Name** drop-down list. The email accounts then fetches the email from the selected poller cluster.

Note:
You must create the poller cluster to select the **Owner Name**.

You can also disable the email account by selecting the **Disable Account** check box.

Outgoing Email Server

The **Outgoing Email Server** tab contains information on how you want to connect your email account with your SMTP server for sending email messages.

To support the SMTP authentication with TLS and secure authentication for an outgoing email communication, the additional fields are provided on this tab.

If an administrator wants to enable the secure communication and SMTP Authentication for the configured email account, the administrator has to select appropriate security options on this tab.

You can specify:

- **Outgoing Email Server (SMTP)**. Outgoing messages (replies from agents) are sent through an SMTP (Simple Mail Transport Protocol) server that is configured to allow connections from your Email Management server system, and from agent systems on your network. Enter the network address for the SMTP server you would like to use here.
- **Outgoing Email Server (SMTP) Port**. The port number which is used by the specified SMTP server.
- **Use TLS**. Click the drop-down list and select the transport layer security (TLS) that you want to use for outgoing emails from this email account. According to the value that you select for TLS, ICManager updates the **Outgoing Email Server (SMTP) Port** field with the default port number for the selected TLS.

  For None and STARTTLS options, the default port number is 25 and for TSL option, the default port number is 465.
- **Use SMTP Authentication**. Select this check box to enable the SMTP authentication for this email account. With this check box selected, the ICEmail server, Website, and ICM Server authenticates the email account every time the agent sends an email from this email account.

  When you select this check box, ICManager makes the following fields visible.

  - Logon account
  - Password
  - Confirm
  - Use Secure Authentication
  - Authentication Type
- **Logon account**. The valid email account name configured on the email exchange server. The ICEmail server, Website, and ICM Server authenticates this account when sending email messages from this email account.
- **Password**. The password for the logon account.
- **Confirm**. The confirmation of the password for the logon account.
- **Use Secure Authentication**. Select this check box to secure the email account password when authenticating the email account. You can select the type of encryption that you want to use to secure the password. By default, ICManager uses the Plain authentication type.

- **Authentication Type**. The SMTP protocol normally uses plain text name and password to log on a user. This means that there is a possibility that a user on the same local area network could intercept and view passwords as they are transmitted between Email Management and the SMTP servers.

  Secure Password Authentication is a challenge-response protocol used by the operating system's security subsystem to prevent passwords from being sent through the network in a plain text format. If the SMTP server supports Secure Password Authentication, and if Email Management is configured to use Secure Password Authentication when logging onto SMTP accounts, the SMTP password will be scrambled rather than being sent as plain text.

  If no authentication type is selected, Email Management will use plain text to send the user ID and password.

- **Test**. The button that you can click to test the specified SMTP server. For details about testing this server, see Testing an email account on page 117. This button is disabled if you select the option **Start TLS** or **TLS** available in the **Use TLS** drop-down option and Use SMTP Authentication option.

Incoming Email Server

The **Incoming Email Server** tab contains information on how this email account should connect to your POP3 and IMAP4 servers to retrieve messages. You can specify:

- **Email Account Type**. You can select POP3 or IMAP4 from the drop-down list. In Avaya IC, you can also use IMAP4 protocol for receiving the emails. In IMAP4, emails will be deleted from the Exchange server once they are processed by an ICEmail server such as POP3. If you select IMAP4, the Mail Folder Name field becomes visible. In this field, you have to enter the name of the folder from which you want fetch the emails.
- **Incoming Email Server**. POP3 or IMAP4 servers require users to log on with a user name and a password in order to retrieve email. Enter the network address of the selected server where the email accounts are configured, the logon account, and password in the appropriate field. If any of these settings are incorrect, Email Management will not be able to connect to the IC Email server. For details about testing this server, see Testing an email account on page 117.
- **Incoming Email Server Port**. This is the port number used by POP3 or IMAP4 servers for receiving mails. 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).
- **Use TLS**. Select this field to enable the TLS (Transport Layer Security) for the emails that are fetched from this email account. For more information, see the *IC Installation and Configuration* guide. 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 enable Authentication Type.

- **Authentication Type**. The POP3 or IMAP4 protocol normally uses plain text name and password to log on a user. This means that there is a possibility that a user on the same local area network could intercept and view passwords as they are transmitted between Email Management and the POP3 or IMAP4 servers.

  Secure Password Authentication is a challenge-response protocol used by the operating system's security subsystem to prevent passwords from being sent through the network in a plain text format. If the POP3 server supports Secure Password Authentication, and if Email Management is configured to use Secure Password Authentication when logging onto POP3 accounts, the POP3 password will be scrambled rather than being sent as plain text.

  If no protocol match takes place, Email Management will use plain text to send the user ID and password.

- **Test**. Click this button to test the email account for incoming mail server.

  If you select the **Use TLS** and **Use SMTP Authentication** options, ICManager disables the Test button.

  For details about testing the incoming server, see Testing an email account on page 117.

Templates tab

The Templates tab lets you specify the following templates:

Header: The text in this template will be inserted at the top of any email to a customer.

Footer: The text in this template will be appended to the end of any email to a customer.

New Message: The text of this template will be automatically sent to a customer when a new email is received from that customer.

Follow Up: The text of this template is sent when a reply is received from a customer or when a follow up email is received from a customer.

Bounce Mail: The text of this template will be automatically sent in response to a message that has been bounced. Avaya IC sends the response to the configured Bounce email address.

To select a template

1. Click the button after the appropriate field. Avaya IC Manager displays the **Select Header Resource** dialog box.
2. Select the **Use Resources** check box.
3. From the **Select Response Library template** section, select the template you want to use.

   The name of the selected template is displayed in the **Name** field.
4. Click **Ok**.

For details about creating templates, see Creating templates on page 93.

Filter tab

You can use the Filter tab to specify the following filter option:

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 come 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 come 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**.

For information about creating filters, see Creating email filters in IC 7.3, 7.3.1, and 7.3.2 on page 123.

Miscellaneous tab

You can use the Miscellaneous tab to specify the following options:

- **Override global email checking scheduler**. Select this check box if you want this email account to check for new messages either more or less frequently than the global setting specified in the **POP3 Cycle wait time** field of the Poller server. For more information about the Poller server settings, see Poller server on page 504.
- **New email check frequency (sec)**. If you have selected Override global email checking scheduler, enter the number of seconds between email checks in this field. The minimum value for this field is 10 seconds. The maximum value that you can set is 999 seconds.
- **Duplicate Message Checking**. Select the check box to enable the checking of duplicate message received by an agent. Selecting these 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 Type** field.
- **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 the check box to enable Blank Email.
- **Blank Email:** The text of this template will be automatically sent to a customer when a blank email (for example, an email with no body text) is received from a customer.
- **Loop Detection Count:** This field specifies the maximum number of acknowledgements that should be sent to a specific customer in any 24 hour period.

Testing an email account

With Avaya IC Manager, you can test the connection to the SMTP server for outgoing email messages and to the POP3 or IMAP4 server for incoming email messages. Using Avaya IC Manager's email account testing functionality, you can send a test message using the SMTP server to find out if the server is running and the email account is working.

To test the outgoing email server

1. In Avaya IC Manager, select **Services** > **Email Accounts**.
2. In the **Email Accounts** dialog box, select an email account for which you want to test outgoing email server.
3. Click **Edit** to display the **Properties** dialog.
4. In the **Properties** dialog, click **Outgoing Email Server** tab.
5. Click **Test**.

   Avaya IC Manager displays the **Email Account Test** dialog box.
6. 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.

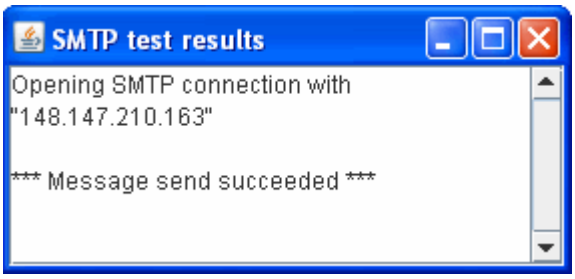
   Avaya IC Manager creates an email with:

   - 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.

   When you click **Test**, it sends that email to the SMTP server. You can use this option to generate multiple test emails and compare the timestamp in their subject lines.

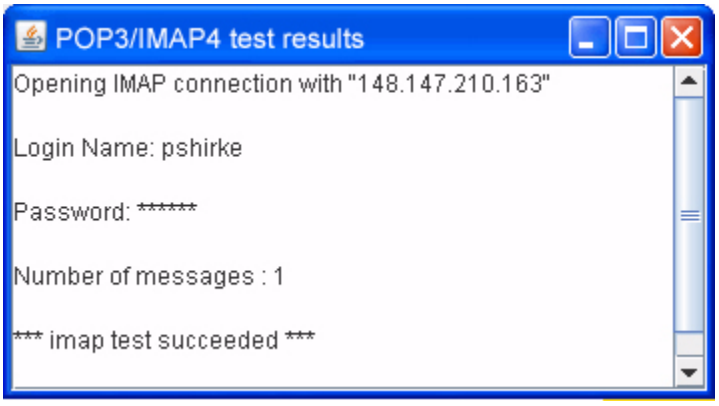
7. Click **Test** to display the **SMTP test results** dialog box.



Important:
If you see any error message in the SMTP connection, check if your antivirus application is restricting the connection. For example, in McAfee antivirus application if the **Prevent mass mailing works from sending mail setting** is enabled, the SMTP connection from ICManager fails.

To test the incoming email server

1. Click the **Incoming Email Server** tab on the **Properties** dialog.
2. Click **Test** to display the POP3 test dialog box.



Configuring email account on Microsoft Exchange for the website to send emails

This section provides information on settings for the account on the Microsoft Exchange server that is used by the website to send the email. Website fails to send an email into the IC system if the website uses an email account configured in the ICManager with SMTP authentication enabled (outgoing email server tab). To use the ICManager with SMTP authentication enabled, the Exchange server requires additional permission for the receive connector used by the website.

Note:
As per Microsoft recommendation, the Exchange server and Domain control must be on different servers.

Settings for Microsoft Exchange 2010

To give additional permission to the account:

1. Identify the email account used by website for sending the email into the IC system (Configured in IC Manager).

   Note:
   This can be identified by looking into the website logs "website_debug.log" with full debug enabled.

   a. Send an email from the website.

   b. Search for the following log snippet:

   ```
   EmailEscalate: sendEmail:: Able to get the email account for the
   emailaddress [@support@ccms.apac.avaya.com : ]
   ```

   Where, support@ccms.apac.avaya.com is <Name>@<Domain> of email account configured in the ICManager.

   c. Identify the configured email account <Name> in the ICManager. The IC Website uses this email account to send the email into the IC system.

2. After identifying the account, the Exchange server requires to set additional permission on the receive connector that the website uses.

   a. Click **Start** > **Exchange Management Shell** and click **Run as Administrator** to run the Microsoft Exchange command shell.

b. To set the permission on the receive connector run the following commands for the IC account:

```
Get-ReceiveConnector "<Machine_Name>\<Receive_Connector_Name>" |
Add-ADPermission -User "<Domain_Name>\<userLogon_Name>"
-ExtendedRights "Ms-Exch-SMTP-Accept-Any-Sender"
```

```
Get-ReceiveConnector "<Machine_Name>\<Receive_Connector_Name>" |
Add-ADPermission -User "<Domain_Name>\<userLogon_Name>"
-ExtendedRights "Ms-Exch-SMTP-Accept-Authoritative-Domain-Sender"
```

For example:

- SANCCMS1.ccms.lab.com = FQDN name for the server hosting the Microsoft Exchange server.
- customer@ccms.lab.com = User Account configured on the Microsoft Exchange server that the IC website uses to send the email.
- Default SANCCMS1 = Receive connector that the IC website uses

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

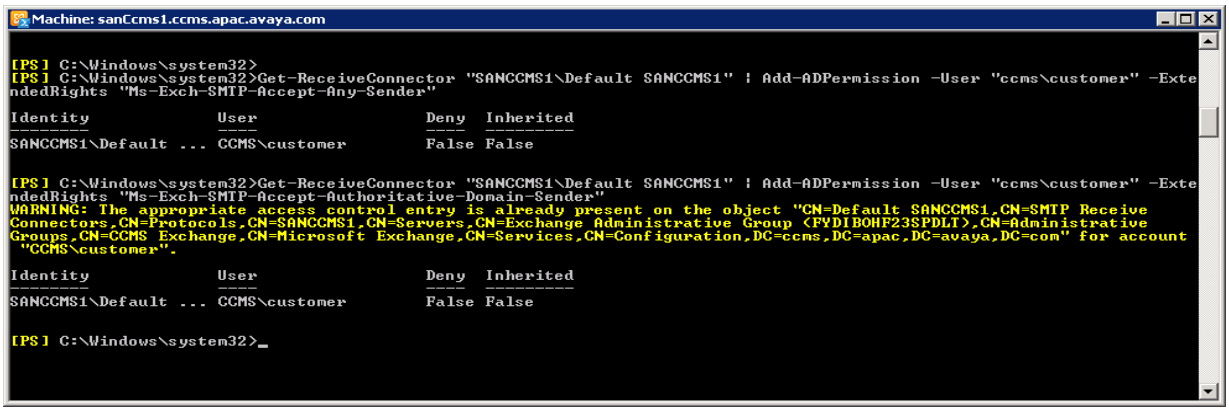
```
Get-ReceiveConnector "SANCCMS1\Default SANCCMS1" | Add-ADPermission
-User "ccms\customer" -ExtendedRights
"Ms-Exch-SMTP-Accept-Authoritative-Domain-Sender"
```

Note:

The permissions are specific to the Receive connector that the website uses. Before running the command ensure that the right receive connector is used. For example, if there is receive connector created other than the default to receive the email from the website then that specific receive connector must be specified in the command. To identify the receive connector, check the smtpreceive logs after enabling the verbose logging. Location for the log is:

```
<Microsoft_Exchange Server_HOME>\V14\TransportRoles\Logs\
ProtocolLog\SmtpReceive
```

c. To verify that the setup is complete, send an email from the website and verify that the received connector name handling the email send by the website (IP of the system hosting the website)



3. Click **Start** > **Run**.
4. In the **Run** window, type **services.msc** and press ***Enter***.
   a. In the **Services** window, right-click the **Microsoft Exchange Transport** service and select **Restart**.
   b. Right-click the **Microsoft Exchange Transport** service and select **Properties**.
   c. Open the **Exchange Management Console**.
   d. In the **Exchange Management Console** window, in the left pane, expand **Microsoft Exchange** > **Microsoft Exchange On-Premises** > **Server Configuration** and select **Hub Transport**.
   e. In the right pane, on the **Receive Connectors** tab, right-click on the Default Exchange 2010 and select **Properties**.
   f. In the **Default Exchange2010 Properties** window, click **Permission Groups**.
   g. On the **Permission Groups** tab ensure that the **Anonymous users** option is selected.
   h. Click **OK**.

Settings for Microsoft Exchange 2013

Exchange server 2013 is more restrictive in terms of the relaying the email. You must provide additional privileges to the user account that the website uses.

1. Click **Start** > **Exchange Management Shell** and click **Run as Administrator** to run the Microsoft Exchange command shell.

2. To set the permission on the receive connector run the following commands for the IC account:

   ```
   Get-ReceiveConnector "<Machine_Name>\<Receive_Connector_Name>" |
   Add-ADPermission -User "<Domain_Name>\<userLogon_Name>" -ExtendedRights
   "Ms-Exch-SMTP-Accept-Any-Sender"
   ```

   ```
   Get-ReceiveConnector "<Machine_Name>\<Receive_Connector_Name>" |
   Add-ADPermission -User "<Domain_Name>\<userLogon_Name>" -ExtendedRights
   "Ms-Exch-SMTP-Accept-Authoritative-Domain-Sender"
   ```

   For example:

   - SANCCMS1.ccms.lab.com = FQDN name for the server hosting the Microsoft Exchange server.
   - customer@ccms.lab.com = User Account configured on the Microsoft Exchange server that the IC website uses to send the email.
   - Default SANCCMS1 = Receive connector that the IC website uses

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

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

   Note:

   The permissions are specific to the Receive connector that the website uses. Before running the command ensure that the right receive connector is used. For example, if there is receive connector created other than the default to receive the email from the website then that specific receive connector must be specified in the command. To identify the receive connector, check the smtpreceive logs after enabling the verbose logging. Location for the log is:

   ```
   <Microsoft_Exchange Server_HOME>\V14\TransportRoles\Logs\
   ProtocolLog\SmtpReceive
   ```

3. To verify that the setup is complete, send an email from the website and verify that the received connector name handling the email send by the website (IP of the system hosting the website)
4. Click **Start**, under **Administrator Tools** select **Active Directory Users and Computers**.
5. In the **Active Directory Users and Computers** window, search for the user account (account created in the exchange for IC) in the Active directory.
6. Right-click the user and select **Properties**.
7. In the **Properties** window, click on the **Member Of** tab.
8. On the **Member Of** tab, assign the user as a member of **Organization Management** group.
9. Click **OK**.
10. Click **Start** > **Run**.
11. In the **Run** window, type **services.msc** and press ***Enter***.

12. In the **Services** window, right-click the **Microsoft Exchange Front End Transport** service and select **Restart**.
13. In the **Services** window, right-click the **Microsoft Exchange Mailbox Transport Delivery** service and select **Restart**.

Email filters

The Email Filters option is a feature of Email Management that lets the administrator define user names or domains that will not be allowed to send messages to Avaya IC email accounts or queues.

There are two types of Email filters:

- VALID_EMAIL_LIST: only the emails with email address that matches the email filter will be routed to your email accounts or queues. If an incoming email address does not match the filter, Email Management forwards the email to the Bounced Message Email Address specified on the General tab of the Email Accounts. Use the VALID_EMAIL_LIST option if there is only a set of email addresses, usernames, or domains that should be able to send messages to your email accounts or queues.
- INVALID_EMAIL_LIST: only the emails with email address that do not match the email filter will be routed to your email accounts or queues. If an incoming email address matches a regular expression pattern mentioned in the filter, Email Management forwards the email to the Bounced Message Email Address specified on the General tab of the Email Accounts. Use the INVALID_EMAIL_LIST option if there is a set of emails addresses, usernames, or domains that should never be able to send messages to any of your Email Management email accounts or queues.

You can filter a complete mailing address, such as "friend@public.com", or on a substring within the email address, such as "@public.com".

- Creating email filters in IC 7.3, 7.3.1, and 7.3.2 on page 123
- Creating email filters in IC Release 7.3.3 and later on page 124

Creating email filters in IC 7.3, 7.3.1, and 7.3.2

To add an email filter:

1. On the **Filter** tab, click the **Ellipses (...)** button for **Accept From** or **Reject From**.

Note:
You can only set either Accept From filter or Reject From Filter. If you set the Accept From filter then the regular expressions defined for Reject From filter will be removed and vice versa.

2. Click **New**.
3. Fill in the address to filter. The following examples show valid email filters:

Filter	Result
friend@public.com	Rejects email from the address *friend@public.com*
friend@	Rejects email from the user name *friend* at any domain.
@public.com	Rejects all email from the domain *public.com.*

4. When you have finished setting up the email filters, click **OK** to save your settings.

If an incoming message matches a filtered address, Email Management forwards the email to the **Bounced Message Email Address** specified on the **General** tab of the Email Accounts.

Creating email filters in IC Release 7.3.3 and later

In IC Release 7.3.3 and later, the administrator can define regular expressions to filter emails that can or cannot send messages to Avaya IC email accounts or queues.

IC 7.3.3 onwards the spam filter no longer automatically rejects emails from email addresses containing the string **`mailer-daemon`** or **`daemon`**. If you want to continue rejecting such emails you must have **daemon** email filter configured.

The Email Management checks an incoming email address for the presence of a substring that matches the regular expression pattern. The default method of pattern matching is case sensitive. You can use regular expression to configure case insensitive pattern of matching.

You can filter a complete email address, such as **friend@public.com**, or a substring within the email address, such as **public.com**.

To add an email filter:

1. On the **Filter** tab, click the **Ellipses (...)** button and select **Accept From** (for VALID_EMAIL_LIST) or **Reject From** (for INVALID_EMAIL_LIST).

   Note:
   You can only set either Accept From filter or Reject From Filter. If you set the Accept From filter then the regular expressions defined for Reject From filter will be removed and vice versa.

2. Click **New**.
3. In the **Add E-mail address** window, type the regular expression to be filtered.
4. Click **OK** to save your settings.
5. When you have finished setting up the email filters, click **OK** to save your settings.

Examples of Filter/Regular Expression

The following examples show valid email filters:

Filter/Regular Expression	Result
^friend@public.com$	Accepts/Rejects emails from the exact address ‘friend@public.com’
friend	Accepts/Rejects emails from any email address which contains the substring friend. For example: • friend@public.com • myfriend@public.com • friend@notpublic.com
^[Ff][Rr][Ii][Ee][Nn][Dd]@[Pp][Uu][Bb][Ll][Ii][Cc].[Cc][Oo][Mm]$	Performs a case insensitive match to Accept/Reject emails from ‘friend@public.com’.
^friend@	Accepts/Rejects all emails from the local part ‘friend@’
@public.com$	Accepts/Rejects all emails from the domain name ‘@public.com’
daemon	Rejects all email which have ‘daemon’ as a substring in the email addresses

If an incoming email address matches a regular expression pattern mentioned in the filter, Email Management forwards the email to the Bounced Message Email Address specified on the General tab of the Email Accounts.

Rogue Wave RWTRegex constructor has been used to define the email filter expressions. For more information see http://docs.roguewave.com/sourcepro/11/html/toolsref/rwtregex.html

Email Filter tool for testing email filter regular expressions

You can use the Email Filter tool to test the regular expressions that you have used for email filtration.

1. On the Design and Admin system, navigate to the ***<AVAYA_IC73_HOME>\bin*** folder.

2. Open the **EmailFilterTool.csv** file.

   The CSV file uses semi-colon as the list separator. If the list separator mentioned in the format settings located under the region and language settings of your system is set to semi-colon, the CSV file will automatically be properly rendered. If not you can either change the list separator to semi-colon on your system or use the text to column feature of the Microsoft Excel under the Data tab and select semi-colon as the delimiter.

   The CSV file has three columns:

   - Filter
   - Email ID
   - Outcome

   In the CSV file, three examples are already provided. To test more regular expressions, type the email filter regular expression string in the **Filter** column that you intend to use in the email manager. For instance type **spam**.
3. In the **Email ID** column, type the expected incoming email address to be tested against the filter.
4. Leave the **Outcome** column empty.
5. Save the CSV file and close it.
6. Run the **EmailFilterTool.exe** application.

After you see the **Action completed please check the 'EmailFilterTool.csv' file for output** message in the command prompt, open the **Email Filter Tool.csv** file and verify the **Outcome** column for the outputs. The results are as follows:

- **Matches** would mean that the regex string entered in the **Filter** column was found in the **Email ID** column.
- **Doesn't Match** would mean that the regex string entered in the **Filter** column was not found in the **Email ID** column.

The tool arranges the final output in the increasing alphabetic order of the filter column.

To test more values, you can add the filters and the email ids to the EmailFilterTool.csv file and run the **EmailFilterTool.exe** application. The values in the Outcome column are automatically updated. You do not require to clear the values from the **Outcome** column.

Note:

- Ensure that the EmailFilterTool.csv file is present in the **`<AVAYA_IC73_HOME>\bin`** folder before running the EmailFilterTool.exe tool.
- Do not overwrite the column names with the filter or email id values as the entry would be lost however the other entries would still be processed.
- Use Microsoft Excel to edit the EmailFilterTool.csv. Using other editors might corrupt the csv file.

Retrieve exact matches in email From address search

To search for messages where an exact match of the From address provided in the search query, configure `FromEmailExact` as 1 on the **Configuration** tab of ICEmail server. After completing the configuration you must restart the ICEmail server.

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

If you configure `FromEmailExact` as 1, the system retrieves messages where the From field is an exact match of the parameter used in the search field.

Note:
You must use the exact From address in the search query for this search option to work.

For example:

If there are two emails with the From address as cust1@xyz.com, and another two emails with the From address as cust1@test.com. If `FromEmailExact` is not configured (default; or != 1), a search of customer email address using `*cust*` in agent client retrieves all the four messages.

If `FromEmailExact=1` is configured, a search of customer email address using `*cust*` does not retrieve any emails. When cust1@test.com is used in the search query, the system retrieves the two emails that contain cust1@test.com in the From address, if they are in the specified time range specified.

For more information about configuring the `FromEmailExact` parameter, see Configuration tab on page 427.

Deleting an email account

To delete an email account:

1. Ensure that the email account that you want to delete does not have any pending emails. If it does, those emails must be reassigned before the account can be deleted.

   Note:
   If you have deleted email tasks for an email account from the WebACD Admin page, you cannot delete that email account.

2. Make sure that the email account is not associated with any FAQ documents. (Avaya IC does not do this check automatically). For more information about working with FAQ documents, see Managing the FAQ database on page 321.
3. Select **Services** > **Email Accounts**.
4. In the **Email Accounts** dialog box, select the account you want to delete.
5. Select **Delete** and confirm the deletion at the prompt.

Failure scenarios for incoming emails

Following are the scenarios during which the incoming emails might result in delivery failure and might bounce:

1. The From address is not present in the configured “Valid Email ID List” for that account.
2. The From address is present in the configured “Invalid Email ID List” for that account.
3. If originator (From/ReplyTo) is empty and DisableRFCCheckInSpamPlugin is false; default.
4. If originator consists of "mailer-daemon" or "daemon".

   Note:
   This failure scenario of originator consisting of "mailer-daemon" or "daemon" is no longer valid from IC 7.3.3 onwards.

5. If originator is invalid and DisableRFCCheckInSpamPlugin is false; default.
6. If the subject consists of the following:
   - "message status - undeliverable"
   - "undeliverable message"
   - "mail system error - returned mail"
   - "undeliverable:"
   - "returned mail: undeliverable"
   - "mail failure"
   - "a message you sent could not be delivered"
   - "ccmail smtplink undeliverable"
   - "delivery failure notification"
   - "delivery notification:"
   - "unresolvable mail address"
   - "automatic reply"
   - "delivery error"
   - "returned mail: user unknown"

Email approval process

You can configure Email Management to send outbound email contacts to an approver for review. To set up an approval process, you need to:

- Create a routing hint for email approval on page 129
- Create an approval workgroup on page 130
- Create an approval queue on page 131
- Create agents for the approval workgroup on page 132
- Configure the IC Email server to analyze outbound emails on page 132

Create a routing hint for email approval

To set up email approval, you must create an approval routing hint for the Set Routing Hint block in the outbound email workflow. Create one of the routing hints described in the following table, depending on whether your Avaya IC system includes Content Analyzer.

Routing hint	Description
approvalrequired	Used for Avaya IC systems that use Analyze with Keyword for email analysis.
suspectcontent	Used for Avaya IC systems that use Content Analyzer for email analysis.

The RoutingHint table must include an email queue that matches the routing hint for email approval and the routing hints found for the original inbound email contact.

For example, an inbound email contact had routing hints for en and sales. The outbound email contact has a routing hint for approvalrequired. The RoutingHint table in the Directory server must include these three routing hints. The three routing hints must be associated with the approval email queue and the same tenant. With this configuration, Email Management can send the outbound email contact to the approval workgroup that is associated with the approval email queue.

For information on the outbound email workflow, see *Avaya IC Media Workflow Reference*. For information on how to create the email approval routing hint, see IC Installation and Configuration.

Create an approval workgroup

To create an approval workgroup:

1. In Avaya IC Manager, select **Tools** > **Groups**.
2. In the **Group Manager** window, double-click **DefaultTenant** in the left pane.

   The Group Manager displays a Default Workgroup in the **Membership** tab on the right pane.
3. Select **Create New Workgroup**.
4. In the **Create New Workgroup** dialog box, complete the fields in the following table:

Field	Recommended entry
Workgroup Name	Enter a name for the approval workgroup. For example, enter ApprovalTeam.
Description	Enter a description of the workgroup.
Notification Method	Select **Owners** from the drop-down list.
Notification Address	Leave this blank.

5. Select **OK** in the **Create New Workgroup** dialog box.

   The Group Manager creates a new workgroup on the same level as the Default workgroup.
6. Select **OK**.

Note:
For more information about workgroups, see Workgroups on page 242.

Create an approval queue

To create an approval queue:

1. In Avaya IC Manager, click the **Device** tab.
2. Select **Device** > **New Device**.
3. In the **New Device** dialog box, select **Email Queue** and click **OK**.
4. In the **Device Editor (Email)** dialog box, click the **General** tab and enter the information for the fields mentioned in the following table:

Field	Recommended entry	Description
Id	Enter the identifier for the queue.	For example, enter approverqueue.
Site	Select the site of your IC Email server.	
Name	Enter a name for the email queue.	For example, enter approverqueue. The name cannot contain: ● Spaces ● More than 32 characters if you want this queue to accept transfers from the Unified Agent Directory.
Priority	Assign a priority to the queue.	For example, enter 1.
Service Level	Enter the number of hours, minutes, and seconds in the format HH:MM:SS	For example, enter 00:30:00 to set thirty minutes as the maximum amount of time that an outbound email should spend in the queue.
Minimum agents	1	Enter the minimum number of agents who must be active to use the queue.
Workgroup	Enter the name of your approval workgroup.	This is the workgroup that you created in Create an approval workgroup on page 130.
Addressable	Check this box if you want the agents to see the queue in the agent directory.	

5. Click **OK**.
6. Select **Manager** > **Refresh**.

Note:
For more information about queues, see Creating devices on page 378.

Create agents for the approval workgroup

You must create at least one agent for the approval workgroup. The agents in this workgroup will be responsible for approving all email contacts marked for approval. For more information, see Creating a new agent on page 216.

Configure the IC Email server to analyze outbound emails

To have the IC Email server analyze all outbound emails, you need to:

1. In Avaya IC Manager, in the list of servers, double-click the IC Email server.
2. Click the **ICEmail** tab.
3. Select the **Run Outbound Email Flow** check box.
4. Click **OK**.

Avaya IC will now run the analyze outbound email workflow that has been uploaded to the Workflow server. For details, see *Avaya IC Media Workflow Reference*.

Enhancements to the Email Templates in IC 7.3.2 FP

The following new parameters have been introduced in IC 7.3.2 FP to enhance the performance of the email templates:

Parameter name	Default value	Description
FolderSize	20 characters	This parameter denotes the size of the string that represents each folder node in the JSON string. This parameter is used to reserve space in the JSON string for better performance. A higher value is recommended if the names of folders are of wider length.
TemplateSize	20 characters	This parameter denotes the size of the string that represents each template node in the JSON string. This parameter is used to reserve space in the JSON string for better performance. A higher value is recommended if the names of templates are of wider length.
StatusSize	20 characters	This parameter denotes the size of the string that represents each status node in the JSON string. This parameter is used to reserve space in the JSON string for better performance. A higher value is recommended if the names of statuses are of wider length.
TemplWriteToFile	0 (false)	If this parameter is true and set to 1, the JSON string sent to agent and other performance parameters are written to AVAYA_IC_HOME/logs/EmailTemplateEncode.log .

Parameter name	Default value	Description
TemplRecreateGenUpd	1 (true)	If this parameter is set to true, the template tree data is recreated from the database upon a GenericUpdate.
AgentTemplateTimeout	500	This parameter denotes the time, in milliseconds, the agent requests for fetching a template tree, waits on the lock before timing out. The minimum value is 500 milliseconds.
FolderBuckets	20 number	This parameter denotes the number of buckets in a hashmap used by template tree to store all nodes. A tree with larger number of nodes should have a higher number of buckets. This tree is the one that is sent to agent and not the tree that represents template data in database. The minimum value is 5.

Chapter 6: Additional configuration options

The Configuration tab for global settings lets you enter additional configuration options for:

- Text chats
- Directory servers
- Telephony servers
- Voice chats
- Tenant websites
- Workflows

To set these options, click the **Configuration** tab in Avaya IC Manager. The left pane shows the available table folders in a tree structure format. Select the symbol next to any table folder to expand that folder and show the tables within it. Select any table, view the records in that table.

The right pane shows either a list of records for the table selected in the tree, the fields contained in the selected record, or when you create a new record, the editable fields for that record.

You can add new records to a table, but you cannot add new tables or table folders.

Out-of-the-box, the **Configuration** tab includes the following table folders and tables:

Table Folder	Tables
Chat	CIRS (Central Internet Routing Service) ICM (Internet Call Manager)
Private Key PassPhrase	Directory Server HTTPConnector Server
Resource Manager	LRM (Logical Resource Manager)
Telephony	ACD Name Link Group TS Group
Voice Chat	IPGateway Voice Media Manager

Table Folder	Tables
Website	Website Context Configuration
WorkFlow	Agent Search RoutingHint VoiceChat

For a list of the default properties associated with these tables, see Default properties on page 138. For details about setting up all of these options, see IC Installation and Configuration.

This section contains the following topics:

- Creating new records on page 137
- Changing records on page 138
- Deleting records on page 138
- Default properties on page 138

Creating new records

To add a record to a table

1. In the left pane of Avaya IC Manager, select a table to which you want to add the record.
2. On the toolbar, click **New Record**.
3. Right-click in the right pane and select **Show Advanced Properties** to view advanced properties.
4. Enter the appropriate information in the fields displayed in the right pane.

   Avaya IC Manager denotes required fields with an asterisk (*).
5. Click **OK** to save your changes or **Cancel** to discard them.

   Avaya IC Manager displays the table updated with new records.
6. Repeat the above steps to add more new records to the currently selected table.

Changing records

To change an existing record

1. In the left pane of Avaya IC Manager, select the table that the record is in.

   If there is only one record in the table, Avaya IC Manager displays it in the right pane. If there are several records in the table, select the appropriate record in the list in the right pane and click **Edit** on the toolbar.
2. Right-click in the right pane and select **Show Advanced Properties** to view advanced properties.
3. Change the appropriate information in the fields displayed in the right pane.

   Avaya IC Manager denotes required fields with an asterisk (*).
4. Click **OK** to save your changes or **Cancel** to discard them.

   Avaya IC Manager displays the table with updated records.
5. Repeat the above steps to updated records from the currently selected table.

Deleting records

To delete a record

1. In the left pane of Avaya IC Manager, select the table that the record is in.

   If there is only one record in the table, Avaya IC Manager displays it in the right pane. If there are several records in the table, select the appropriate record in the list in the right pane.
2. On the toolbar, click **Delete**.
3. Click **Apply**.

Default properties

Out-of-the-box, the **Configuration** tab includes standard and advanced properties for the records within each table. To view the advanced properties

1. Select an existing record or create a new record.
2. Right-click in the right pane and select **Show Advanced Properties**.

This section contains the following topics:

- Chat table folder on page 139

- Private Key PassPhrase table folder on page 144
- Resource Manager table folder on page 145
- Telephony table folder on page 145
- Voice Chat table folder on page 146
- Website table folder on page 148

Chat table folder

The Chat table folder contains the CIRS and ICM tables.

CIRS record properties

The CIRS servlet is a load-balancing servlet for Web Management that is used if you have multiple ICM servers. Records in the CIRS table can have the following properties (to view the advanced properties listed below, right-click and select Show Advanced Properties from the pop-up menu):

Property Name	Description
Global CIRS Name	Enter the name of the CIRS. The CIRS server uses this parameter to determine which CIRS record to read for configuration. Must match the `dsObject` parameter in the `etc/cirsSystemParms.txt` file.
CIRS Active	Select this check box if the CIRS is active. External clients use this parameter to determine which ICMs to use.
IC Site	Select the Avaya IC site that this server is associated with.
Advanced Properties	
CIRS Servlet Port	Enter the CIRS port number. For a list of default port numbers for components in Avaya IC, see IC Installation and Configuration.
CIRS Hostname	The name and domain of the machine that hosts the CIRS server. For example, `TESTBOX.xyzcorp.com`.
CIRS Port	Enter the port number. For a list of default port numbers for components in Avaya IC, see *IC Installation Planning and Prerequisites*.
No Resource URL	Enter the URL used if no resources are available.
Util Port	Enter the port number. For a list of default port numbers for components in Avaya IC, see *IC Installation Planning and Prerequisites*.

ICM record properties

Records in the ICM table can have the following properties (to view the advanced properties listed below, right-click and select **Show Advanced Properties** from the pop-up menu):

Note:
These properties are options. The out-of-the box ICM can still operate without configuring these options.

Property Name	Description
Global ICM Name	Enter the name for the ICM server. The server uses this parameter to determine which ICM record to read for configuration. Must match the `dsObject` parameter in the `etc/systemParms.txt` file.
ICM Active	Select this check box if the ICM is active. External clients use this parameter to determine which ICMs to use.
ICM Server Name	Enter the fully-qualified domain name of the machine that hosts the primary ICM server.
SMTP Host	Enter the fully qualified domain name of the machine 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	Enter the directory where Avaya IC stores the chat transcripts.
Style Sheet Directory	Enter the directory where Avaya IC stores the style sheets used to format emails that include chat transcripts.
CIRS Host	Enter the name of the machine that hosts the CIRS server used for load balancing.
ICM Property Management Debug Level	Select a number from 0 to 4, where 0 is the lowest level of logging and 4 is the highest.
ICM Toolkit Debug Level	Select a number from 0 to 4, where 0 is the lowest level of logging and 4 is the highest.
ICM Debug Level	Select a number from 0 to 4, where 0 is the lowest level of logging and 4 is the highest.

Property Name	Description
Use Local Timestamps in Chat Transcript	Select this option to store the chat transcripts with local timestamps in the database. If you clear this checkbox, the system stores the chat transcripts in the UTC format in the database. By default, the UTC format is used.
Advanced Properties	
Agent Connectivity Options	Enter three sets of seconds separated by spaces. For example, enter 60 600 1200 Represents the following parameters for configuring agent connections in seconds: ● checkInterval. How often to check the state of the connections. ● sendInterval. How often to send a `keepalive` event across the connection. ● disconnectInterval. How long to wait before disconnecting a connection due to no response to normal or `keepalive` messages across the connection. **Note:** Avaya recommends the use of the following formula to define these values: disconnectInterval >= checkInterval + sendInterval + X * checkInterval. In systems with low load X = 1. In systems with high load X = 6.
CIRS Connectivity Options	Enter three sets of seconds separated by spaces. For example, enter 60 600 1200 Represents the following parameters for configuring CIRS connections in seconds: ● checkInterval: How often to check the state of the connections. ● sendInterval: How often to send a `keepalive` event across the connection. **Note:** Avaya recommends the use of the following formula to define these values: disconnectInterval >= checkInterval + sendInterval + X * checkInterval. In systems with low load X = 1. In systems with high load X = 6.

Property Name	Description
Caller Connectivity Options	Enter three sets of seconds separated by spaces. For example, enter 60 600 1200 Represents the following parameters for configuring caller connections in seconds: ● checkInterval: How often to check the state of the connections. ● sendInterval: How often to send a `keepalive` event across the connection. **Note:** Avaya recommends the use of the following formula to define these values: disconnectInterval >= checkInterval + sendInterval + X * checkInterval. In systems with low load X = 1. In systems with high load X = 6.
ICMBridge Connectivity Options	Enter three sets of seconds separated by spaces. For example, enter 60 600 1200 Represents the following parameters for configuring ICMBridge connections in seconds: ● checkInterval: How often to check the state of the connections ● sendInterval: How often to send a `keepalive` event across the connection **Note:** Avaya recommends the use of the following formula to define these values: disconnectInterval >= checkInterval + sendInterval + X * checkInterval. In systems with low load X = 1. In systems with high load X = 6.
IC Site	Select the Avaya IC site that this server is associated with.
Transcript Poll Interval	Use the up and down arrows to select the desired number of minutes. This parameter specifies how long the ICM server waits before checking the chat transcript directory and processing the transcripts to email to customers and save to the database.
CIRS Host	Enter the host name for the CIRS server.
CIRS Port	Enter the port number. For a list of default port numbers for components in Avaya IC, see *IC Installation Planning and Prerequisites*.

Property Name	Description
PDM Path	Enter the directory and file name of the PDM.xml file.
Attribute Server	Select the Attribute server from the drop-down list.
Maximum Property Management Log Size	Enter the desired size for the ICM website integration log, named: `icmname_website.log`
Tunnel Port	Enter the port number. For a list of default port numbers for components in Avaya IC, see IC Installation and Configuration. To enable tunnelling 1. Go to the system that hosts the ICM server. 2. Open the `callerap.txt` file in an ASCII editor, such as Notepad. 3. Ensure that the `$tunnelEnabled$` parameter is set to `True`.
Agent Server Port	Enter the port number. For a list of default port numbers for components in Avaya IC, see *IC Installation Planning and Prerequisites*.
Caller Port	Enter the port number. For a list of default port numbers for components in Avaya IC, see *IC Installation Planning and Prerequisites*.
Util Port	Enter the port number. For a list of default port numbers for components in Avaya IC, see *IC Installation Planning and Prerequisites*.
Enable Transcript Added Flow	Select this check box only if your Avaya IC system includes integration with another system. When you select this check box, the ICM server runs the workflow from the Transcript Added Flow Name field when Avaya IC processes chat transcripts.
Transcript Added Flow Name	Name of the workflow to run when Avaya IC processes the chat transcript. Use the format `project_name.flow_name` in this field. Avaya IC does not include a sample transcript added workflow.
Transcript Added Flow Event	Name of the event to send in a WorkFlow.Run request when the server processes the chat transcript. **Note:** You do not need to set this parameter to run an `icm.transcriptadded` workflow. This parameter is only required if additional event data is needed in the workflow.

Property Name	Description
Validate URL	Select the Validate URL option to enable verification of URL that the customer sends to the Agent over the Chat or the URL that the Agent sends to the customer. This option uses regular expression for validation. The agent or customer will receive the chat content as text if the customer sends: ● URL with text ● Multiple URL ● URL with space
URL Validation Regex	The URL Validation Regex field defines the Regular Expression that is used to validate the URL when the Validate URL option is enabled. Leave this field blank to set the default regular expression, which is defined as follows: ^((https?\:\/\/)?|www\.)([\w\-_]+(?:(?:\.[\w\-_]+)+))([\w\-\.,@?\^=%&:\/~\+#()']*[\w\-\@?\^=%&\/~\+#)])?$ You can define custom regular expression that can be used for validating the URL.

Private Key PassPhrase table folder

The Private Key PassPhrase table folder contains the Directory server and HTTPConnector server tables.

In the Private Key PassPhrase table folder, you can configure the passphrase protection to the SSL certificate private key for the Directory server and HTTPConnector server.

Directory Server record properties

Records in the Directory Server table can have the following properties (to view the advanced properties listed below, right-click and select **Show Advanced Properties** from the pop-up menu):

Property Name	Description
Directory Server	Enter the name of the Directory Server. The Directory Server uses value of this parameter to determine from which Directory Server the configuration to read.
Password Phrase	

HTTPConnector Server record properties

Records in the HTTPConnector Server table can have the following properties (to view the advanced properties listed below, right-click and select **Show Advanced Properties** from the pop-up menu):

Property Name	Description
HTTPConnector Server	Enter the name of the HTTPConnector Server. The HTTPConnector Server uses value of this parameter to determine from which HTTPConnector Server the configuration to read.
Password Phrase	Enter the PassPhrase that you specified when creating the certificate.

Resource Manager table folder

The Resource Manager folder lets you define the LRMs needed for Business Advocate. For details, see *IC Business Advocate Configuration and Administration*.

Records in the LRM table can have the following properties:

Property Name	Description
Name	The alphanumeric name of the LRM. (You cannot use spaces or special characters.)
Description	A description of the LRM.

Telephony table folder

The Telephony table folder contains the ACD Name, Link Group, and TS Group tables.

ACD Name record properties

Records in the ACD Name table can have the following properties:

Property Name	Description
ACD Name	The alphanumeric name of the ACD. (You cannot use spaces or special characters.)

Link Group record properties

Records in the Link Group table can have the following properties:

Property Name	Description
Name	The alphanumeric name of the link group. (You cannot use spaces or special characters.)
Description	A description of the link group.
Group	The Telephony servers that handle the CTI link to the group table in Avaya IC. All servers in the link group must have the same ACD name and belong to the same switch. Do not create a link group that includes Telephony servers that belong to more than one switch. For details about link groups, see *IC Business Advocate Configuration and Administration*.

TS Group record properties

Records in the TsGroup table can have the following properties:

Property Name	Description
Name	The name of this group of Telephony servers.
Group	Click the button to display the Group dialog box where you can add or remove Telephony servers from the current group.

Voice Chat table folder

The Voice Chat table folder contains the IPGateway and Voice Media Manager tables.

IPGateway record properties

Records in the IPGateway table can have the following properties:

Property Name	Description
Name	The alphanumeric name of the gateway.
IP Address	The IP address for the gateway.

Property Name	Description
Port	The port for the gateway. For a list of default port numbers for components in Avaya IC, see *IC Installation Planning and Prerequisites*.
ACD Name	The name of the ACD file associated with this gateway.
Site	The Avaya IC site associate with the gateway.
Route Point	The dialable number that the gateway uses to route calls.
Capacity	The maximum number of supported calls. This value must be less than or equal to 31.
Active	Select this check box if the gateway is active.

Voice Media Manager record properties

The Voice Media Manager (VMM) serves as a proxy between the VoIP applet and the gateway. Records in the Voice Media Manager table can have the following properties:

Property Name	Description
Name	The alphanumeric name of the VMM.
IP Address	The IP address for the VMM.
Port	The port for the VMM. For a list of default port numbers for components in Avaya IC, see *IC Installation Planning and Prerequisites*.
Site	The Avaya IC site associate with the VMM.
Active	Select this check box if the VMM is active.

Website table folder

The Website table folder contains the Website Context Configuration table. Records in this table can have the following properties:

Property Name	Description
Global Name	Enter the global name (for example, `website`). The ICM server uses this parameter to determine which ICM record to read for configuration. Must match the `dsObject` parameter in the `etc/systemParms.txt` file
Context Active	Select this check box if external clients should use this configuration. This box must be checked for the Website to function.
CIRS Name	Enter the name of the CIRS server to which the ICM CIRS servlet connects to perform load-balancing for chat contacts.
Website Debug Level	Select a number from 0 to 4, where 0 is the least level of logging and 4 is the greatest level.
Default hostname for context	Enter the name of the machine that hosts the website. This name is 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 *`machine_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 will be `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. It is 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 will be: `http://<hostname>/support/public`

Property Name	Description
Default internet protocol	Select a protocol from the drop-down list. Used by external clients to determine website protocol.
Default port for context	Enter the default port number for the website's HTTP connection. For a list of default port numbers for components in Avaya IC, see IC Installation and Configuration.
Advanced Properties	
Admin Pages Active	Select this check box if the administration pages should be accessible.
Public Pages Active	Select this check box if the public pages should be accessible.
Maximum website debug file length	Enter the maximum file size.
Toolkit Debugging Level for Website	Select a number from 0 to 4, where 0 is the least level of logging and 4 is the greatest level.
Path to PDM metadata file	Enter the directory path and file name of the PDM XML metadata file. The default path and file name are: `IC_INSTALL_DIR\etc\pdm.xml`
Attribute Server	Select the Attribute server from the drop-down list. This is the Attribute server to which the website connects to send or receive property management and self-service FAQ updates. If you leave this blank, the Website tries to locate the Attribute server.
Heartbeat Enabled	Select this option to have the client send periodic "Keep Alive" messages to the server.
Heartbeat Interval	The length of time that should pass between "Keep Alive" messages if the Heartbeat Enabled parameter is selected.
Heartbeat Timeout interval	The length of time the client should wait for a response from the server before the client assumes the server has shut down.

WorkFlow table folder

The WorkFlow table folder contains the Agent Search, RoutingHints, and Voice Chat tables. For details about workflows, see *Avaya IC Media Workflow Reference*. For details about configuring these properties, see IC Installation and Configuration.

Agent Search record properties

Records in the Agent Search table can have the following properties:

Property Name	Description
Name	The "update_agentstate_cache" flow under the project "sys_agentsearch" updates the cache of the state of all agents in the system if the time interval for such an update request is more than 600 seconds. If this time interval has to be overridden, this property could be used to set the name of the configuration parameter the flow should look into for overriding the default time interval of 600 seconds. After setting this property, the "update_agentstate_cache" flow must be modified to look into this property value.
Value	An integer representing the time interval (in seconds) between two subsequent updates of the cache of the state of all agents in the system. If this value is set to 0, the agent state cache update will be stopped.

RoutingHint record properties

For details about creating Routing Hints, see IC Installation and Configuration. For information about implementing Routing Hints, see *Avaya IC Media Workflow Reference*.

Records in the RoutingHint table can have the following properties:

Property Name	Description
Routing Hint	A hint for routing a contact. For a: • Voice contact, a DNIS or an ANI is a valid hint. • Chat contact, the hint must be Routing Hint associated with an FAQ document (For more information, see Managing the FAQ database on page 321.) • Email contact, the hint must be a routing hint that would be determined on analyzing an email either by a keyword search or by using the Content Analysis server. **Tip:** To specify a queue as a routing hint, enter the information found in the ID column on the Device tab.
Voice Queue Id	A valid voice queue ID (or Device number) to which the hint specified in the Routing Hint property must be mapped. **Tip:** You can find the voice queue ID in the Queue ID column on the Device tab.
Chat Queue Id	A valid chat queue ID (or Device number) to which the hint specified in the Routing Hint property must be mapped.
Email Queue Id	A valid email queue ID (or Device number) to which the hint specified in the Routing Hint property must be mapped.
Category/Qualifier	The category or qualifier for the Routing Hint. **Note:** This field is reserved for use by Business Advocate in Avaya IC.
Tenant	The tenant that this routing hint applies to.
Advanced Properties	
User Defined	Advanced users of the system may use this property to map any value to the specified Routing Hint.

VoiceChat record properties

Records in the VoiceChat table can have the following properties:

Property Name	Description
Name	Enter the name of the IV chat flow.
TImeout	Enter 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.

Configuring LDAP

Lightweight Directory Access Protocol (LDAP) provides **single sign on** facility where one password for a user is used between multiple enterprise applications. IC 7.3 supports LDAP.

To successfully enable LDAP support with Avaya Interaction Center, you must configure the LDAP as per the procedure given in this chapter.

Along with addition of LDAP support in IC, a change was made to enable SSL communication between IC clients and directory server, for example, the clients sending requests to directory server like DS.Login or DS.Authenticate requests will go over SSL.

Note:

- To enable SSL communication between IC server and clients, Avaya provides self signed certificate which is installed by default on the system. You can replace these certificates with the CA authority certificates.
- LDAP support for IC is tested using Microsoft's Active Directory implementation on Windows platform and OpenLDAP implementation on Unices. The procedure in this chapter refers to the Active Directory and OpenLDAP implementations. Therefore, LDAP server refers to Active Directory or OpenLDAP server.
- When LDAP is enabled, a single Directory Server can authenticate client requests against LDAP and Non-LDAP.

The following sections provide detailed information about configuring the required Avaya Interaction Center components for the LDAP support.

Configure the following components in the given order.

1. Directory Server on page 152
2. Design and Admin on page 154

Directory Server

The Directory Server communicates with the LDAP server for authenticating login credentials of LDAP users. Directory server can communicate with the LDAP server in SSL or non-SSL mode. Directory Server works as a client for LDAP server.

LDAP server certificate for SSL communication

You must ensure that the Directory Server trusts the LDAP server if the Directory Server is connecting to LDAP over SSL. To enable SSL communication between Directory Server and LDAP Server, you must install the LDAP Server certificate or the certificate from the Certificate Authority (CA) on the Directory Server system. The Directory Server can trust the certificate coming from LDAP server during SSL handshake by comparing the certificate with the installed certificate.

Installing the LDAP server certificate from the Certificate Authority to the Directory Server is described below for Windows, Solaris, and AIX platforms.

Directory Server running on Windows

If you have configured the Directory Server on Windows, you must install the LDAP server certificate from CA in the Windows certificate store of a system, where Directory Server is running. If you configured multiple Directory Servers, you must install the LDAP server certificate from CA in the Windows certificate store of each system where Directory Server is configured and running.

You can also import the certificates from CA to the Windows certificate store if the certificates are PEM-encoded and the certificate file has the .cer extension.

When you create a secure connection to the LDAP server, the SSL library selects the appropriate CA certificate to sign the certificate presented by the LDAP server. In this case, you can keep the certificate field specified in the LDAP server configuration blank.

Directory Server running on UNIX

If you have configured the Directory Server on any of the IC supported UNIX platforms (Solaris or AIX), you must save the LDAP server certificate from CA in the encoded PEM format on the file system. During the LDAP server configuration, you must specify the certificate filename in the **Certificate Name** field and also copy the certificate to the `AVAYA_IC73_HOME/etc` directory on a system where Directory Server is running. If you have configured multiple Directory servers, you must perform this procedure for every Directory server.

Note:

Ensure that value in the **LDAP Server Name** field specified in the LDAP server configuration matches with the hostname specified in the **commonName** field of the LDAP server certificate. If the values do not match, the SSL handshake between Directory Server and the LDAP server will not be successful. Also, the LDAP server authentication for users will not work.

Design and Admin

Importing the LDAP server certificate to IC Manager

The Directory Server communicates with the LDAP server for authenticating login credentials of LDAP users. IC Manager communicates with the LDAP server for importing and synchronizing LDAP users to the IC system. IC Manager can communicate with the LDAP server over the SSL and non-SSL modes.

IC Manager works as a client for LDAP server and you must ensure that IC Manager trusts the certificate of the LDAP server if IC Manager is connecting to LDAP server over SSL. For SSL communication between IC Manager and LDAP Server, you must install the LDAP Server certificate or the certificate from the CA to trusted certificates store of JRE. Ensure that the JRE is the JRE used by IC Manager. After this, IC Manager can trust the certificate coming from LDAP server during SSL handshake by comparing the certificate with the installed certificate.

Note:

From IC 7.3.2 onwards, there must be only a single instance of JRE and that must not be lower than 1.6.0_45. Users who have JRE already installed must upgrade to JRE 1.6.0_45. There will be no prompt from the system to upgrade to the required version. However, if there is no JRE installed, the system will automatically install JRE version 1.6.0_45.

Perform the following steps to install the signing authority (CA) credentials, which has signed the certificate of LDAP server trusted certificates store of JRE.

To install the certificate:

1. Copy the LDAP Server certificate or the certificate from the Certificate Authority (CA) from LDAP server system to the *IC_INSTALL_DIR*`\Java\lib\security` directory on the IC Design and Admin system.
2. Rename the certificate to `root_cert_LDAP_server.pem`.
3. To import the above certificate, go to the command prompt and run following commands:
   - **cd** *IC_INSTALL_DIR*`\Java\lib\security`
   - *IC_INSTALL_DIR*`\Java\bin\keytool.exe -import -file root_cert_LDAP_server.pem -alias <Certificate Unique Alias Name> -keystore jssecacerts -storepass changeit`
4. Verify that the `jssecacerts` keystore is present in *IC_INSTALL_DIR*`\Java\lib\security` directory in the form of a file.
5. Check if the `root_cert_LDAP_server.pem` file is successfully imported to `jssecacerts` keystore using the following command:
   - *IC_INSTALL_DIR*`\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 you changed.

All keystore entries (key and trusted certificate entries) are stored and accessed through unique, case-insensitive aliases through the keystore. If there is no alias name to the certificate, keytool uses the default alias name `mykey`.

Enabling the LDAP menu in IC Manager

You can enable the LDAP integration support by configuring the **EnableLDAP** property in IC Manager. After you configure the **EnableLDAP** property in IC Manager, you can view the **LDAP** menu in IC Manager. Avaya IC communicates with LDAP only if you set the **EnableLDAP** property value to **Yes**.

Perform the following steps to configure the **EnableLDAP** property to IC Manager.

1. In IC Manager, on the main menu, click **Tools** > **Groups**.
2. In the **Group Manager** dialog box:
   a. In the left pane, click **IC**.
   b. Click the **Properties** tab.
   c. In the Sections field, click System/Configuration.
   d. In the **Settings** pane, click the **Assign Property** button on the toolbar.
   e. In the **Assign Property** dialog box:
      1. Click the **Property** field and select **EnableLDAP**.
      2. Click the **Property Value** field and select **Yes**.
      3. Click **OK**.
   f. Click **OK**.
3. In IC Manager, on the main menu, click **File** > **Exit**.
4. Restart IC Manager.
5. Log in to IC Manager as an administrator.
6. On the main menu, click **Services** to view the **LDAP** menu.

Configuring the LDAP server properties

IC Manager communicates to the LDAP server for importing and synchronizing the LDAP users in the Avaya IC system. Similarly, the Directory server communicates with the LDAP server for authenticating users.

Perform the following steps to store the LDAP configuration details, which IC Manager or Directory server can use.

To configure the LDAP server properties:

1. In IC Manager, on the main menu, click **Services** > **LDAP** > **LDAP Configuration**.
2. In the LDAP Configuration dialog box, click **New** to create a new LDAP configuration.
3. In the **New LDAP Configuration** dialog box, enter the field values as explained in the below table:

Field	Description
LDAP Server Name	The host name or IP address of the LDAP server system.
LDAP Server Port	The port number at which the IC Manager or the Directory server communicates with the LDAP server. Default non-SSL port number: 389 and Default SSL port number: 636.
Base DN	The base distinguished name of the LDAP server. For example, dc=ldap,dc=com.
SSL Enabled	The check box to select if you want to set the communication between IC system and LDAP over SSL.
Certificate Name	The certificate name of the LDAP server. The Directory server uses the default value only for the UNIX platform. For Windows platform, you can specify the different value.

4. Click **OK**.
5. Click **OK** in the **LDAP Configuration** dialog box.

Note:
Only one Active Directory/LDAP configuration creation is supported with IC. Thus after saving first Active Directory/LDAP Configuration, the New button will be disabled in LDAP Configuration dialog box.

Verifying the LDAP configuration

After you configure the LDAP server properties in IC Manager, you can verify if the configuration is correct and validate the provided configuration data.

To verify the LDAP configuration:

1. In IC Manager, on the main menu, click **Services** > **LDAP** > **LDAP Configuration**.

2. In the LDAP Configuration dialog box:
   a. Select the LDAP Configuration that you want to verify and validate.
   b. Click **Edit**.
3. In the **Edit LDAP Configuration** dialog box, click the **Verification** tab.
4. In the **LDAP DN** field, enter the LDAP distinguished name.
5. In the **Password** field, enter the password.
6. Click **Test**.

   The system will test the connection with the LDAP server using the specified distinguished name and password, and display a message box about the result.

Mapping the employee table fields from the Avaya IC database with the LDAP user attributes

To import or synchronize the LDAP users in to the Avaya IC system, you need to first map the fields from the employee table in the Avaya IC repository database with the LDAP user attributes.

While importing or synchronizing the LDAP users in to the Avaya IC system, the mapped LDAP user attributes are populated into the corresponding columns of employee table of the Avaya IC repository database.

IC Manager saves the fields mapping along with the LDAP configuration in the `ldapconfig` table.

IC Manager first reads the LDAP user attributes and fields from the `employee` table in the IC database from the `agentAttributes.xml` file located in the `IC_INSTALL_DIR\etc\` directory. After reading the information from the `agentAttributes.xml` file, IC Manager displays the fields in the following columns in the **IC-LDAP Map** dialog box.

- IC Fields

  In this section the IC fields are specified as XML tags. The tag name represents the actual IC field name in the `employee` table of the IC repository database and the value inside the tag represents display name of that IC field.

  The following code snippet shows the fields from the `employee` table and their display name.

```
<Snippet>
.
.
.
<ICFields>
  <loginname>Login Name</loginname>
  <firstname>First Name</firstname>
  <lastname>Last Name</lastname>
  <fullname>Full Name</fullname>
  <preferredname>Preferred Name</preferredname>
  <userDN>User DN</userDN>
</ICFields>
.
.
.
</snippet>
```

  In the code snippet, the tag name `<loginname>` represents the actual IC field name in the employee table and the value `Login Name` represents the display name in the **IC-LDAP Mapping** dialog box.

Note:

Before you map the IC fields with the LDAP user attributes, you must check the installed `agentAttributes.xml` file and verify that the LDAP schema has all the user attributes present as defined in the LDAP Fields column.

- LDAP Fields

  In this section the LDAP user attributes are specified as XML tags. The tag name represents the actual LDAP user attribute name and the value inside the tag represents the display name of that user attribute.

  The following code snippet shows the LDAP user attributes and their display name.

```
<Snippet>
.
.
.
<LdapFields>
  <sAMAccountName>sAMAccountName</sAMAccountName>
  <givenName>Given Name</givenName>
  <sn>Last Name</sn>
  <distinguishedName>Distinguished Name(AD)</distinguishedName>
  <!-- This must be used for Active Directory systems. -->
  <entryDN>Entry DN(OpenLDAP)</entryDN>
  <!-- This must be used for OpenLDAP systems. -->
</LdapFields>
.
.
.
</Snippet>
```

  In the code snippet, the tag `<givenName>` represents the actual user attribute name of the LDAP user and the value `Given Name` represents the actual display name in the **IC-LDAP Mapping** dialog box.

  Important:
  There must be one LDAP user attribute that has a unique value associated with it across the LDAP server users. You must map this attribute with the `loginname` field in the IC fields. The other user attribute, such as `DN` needs to mapped with the `userDN` field in the IC Fields.

  The LDAP user attribute names can vary depending upon the LDAP server type. For example, the attribute name `distinguishedName` in Active Directory is called as `entrydn` in OpenLDAP.

Importing users from the LDAP server

In IC Manager, you can import the LDAP users to the Avaya IC system based on the fields mapping you did on the **IC-LDAP Map** dialog box. For more information about mapping fields, see Mapping the employee table fields from the Avaya IC database with the LDAP user attributes on page 157.

To import user from the LDAP server:

1. In IC Manager, on the main menu, click **Services** > **LDAP** > **LDAP Import**.
2. In the **Import LDAP users** dialog box:

a. In the **LDAP DN** field, enter the LDAP distinguished name (DN), which has permission to search users in the LDAP server.

b. In the **Password** field, enter the password for the specified DN.

c. Click **Login**.

   Based on the successful login, the system displays the Import users screen.

d. Click the check box corresponding to the user that you want to import.

   (OR) Click the **Select all** check box to select all the configured LDAP users.

e. Click **Import**.

   The system starts importing the selected LDAP users and displays the import status of each selected LDAP user.

f. Click **Finish**.

3. After importing the LDAP users you must go to IC Manager.

   a. In the IC Manager, click **Agent** tab.

   b. In the **Agent** tab, select all the imported LDAP users and press **Shift+Control+Right-click** to launch multi-agent edit window.

   c. In the right-click option click **Edit**.

   d. In the **Multi Agent Edit** window, on the **Agent** tab, under **Membership Information**, change the **Domain** option from LDAPuser to the IC User domain.

   e. Click **Apply**.

   f. Click **Ok**.

Specifying the search criteria

When you import the configured LDAP users to the Avaya IC system, you can specify a criteria to search the specific LDAP users.

The **Import LDAP users** dialog box contains a text field to specify the search criteria and a button to search the LDAP users.

While specifying the search criteria, you must follow the LDAP query creating rules.

For example:

- Query string for the list of users belonging to division *rnd* is: `(division=rnd)`
- Query string for the list of users who do not belong to *rnd* and have an email ID is: `(&(!(division=rnd))(mail=*))`
- Query string for the list of users whose name begins with *agent* is: `(name=agent*)`

Synchronizing LDAP user attributes with the Avaya IC system

On the LDAP server, if the attributes of the users, which you already imported in the Avaya IC system, are changed, you need to synchronize the attributes of such users with the Avaya IC system.

To synchronize LDAP user attributes with the Avaya IC system:

1. In IC Manager, on the main menu, click **Services** > **LDAP** > **LDAP Synchronization**.
2. In the **Synchronize LDAP users** dialog box:
   a. In the **LDAP DN** field, enter the LDAP distinguished name (DN), which has permission to search users in the LDAP server.
   b. In the **Password** field, enter the password for the specified DN.
   c. Click **Login**.
   d. Click **Start Synchronization**.

      The system start synchronizing the LDAP user attributes with the Avaya IC system and displays the synchronization status of each LDAP user.

   Note:
   After the synchronization process is complete, the system disables the **Start Synchronization** button.

   The system starts importing the selected LDAP users and displays the import status of each selected LDAP user.

   e. Click **Finish**.

      The system enables the **Finish** button only after the LDAP user attributes are successfully synchronized with the Avaya IC system.

Changing the password management options

Avaya IC system does not manage the passwords for the LDAP users in IC-LDAP integration. Avaya IC sends the user-password and a unique identifier (usually the Distinguished Name of the user) to the LDAP server for authenticating the LDAP user. After the receiving the authentication result from the LDAP server, Avaya IC system passes that result to the respective clients.

To avoid the confusion of managing passwords of the LDAP users, you must turn off the password management configurations of the Avaya IC system.

To change the password management options for LDAP users:

1. In IC Manager, on the main menu, click **Tools** > **Property Declaration**.
2. In the **Property Declarations** dialog box:
   a. In the **Property Section** field, click **AgentSecurity**.
   b. In the **Props for Agent/Security section** field, click **PasswordChange**.

c. In the **Applicable Property Levels** field, select the level at which you want to change the password management options:

d. Click **OK**.

3. In IC Manager, on the main menu, click **Tools** > **Groups**.

   The system displays the **Group Manager** dialog box.

4. In the **Group Manager** dialog box:

   a. In the left pane, click **IC**.

   b. Click the **Properties** tab.

   c. In the **Sections** field, click **AgentSecurity**.

   d. In the **Settings** pane at the right side, double-click **PasswordChange**.

      The system displays the **Edit Property PasswordChange** dialog box.

   e. Click the **Property Value** field and select **No**.

      For LDAP users, if you set the **PasswordChange** option of Agent/Security to **Yes** the respective agent gets an option to change the password from the Avaya IC client application. But the LDAP user, changing the password from the Avaya IC client application does not actually change the password maintained at the LDAP server. So, agents can confuse when they try to use the new password changed from the Avaya IC client application, which the Avaya IC client will not accept.

      For the LDAP users, Avaya IC does not use the values of following password management options:

      - Agent/Security > MinPasswordAlphabets
      - Agent/Security > MinPasswordLength
      - Agent/Security > MinPasswordNumerics
      - Agent/Security > NumOfDays
      - Agent/Security > NumOfPasswordChanges
      - Agent/Security > PasswordChangeDuration
      - Agent/Security > PasswordReuseCycles

      In addition to above properties, the following fields on the **Security** page of the user properties dialog box are disabled for the users imported from the LDAP server:

      - Password
      - Confirm
      - Force password change on login

   f. Click **OK**.

   g. In the **Group Manager** dialog box, click **OK**.

Login attempts for the LDAP users

To control the login attempts to the Avaya IC system, the Avaya IC system refers the **Agent/Security** > **MaxLoginAttemptsAllowed** property value that you set in IC Manager. Avaya IC system refers this value in a same way for internal Avaya IC users and users imported from the LDAP server.

For example:

- For an imported LDAP user, **MaxLoginAttemptsAllowed** property is set to 3 in the Avaya IC system and 5 on the LDAP server.

  After 3 unsuccessful login attempts to the IC system, Avaya IC disables the login for that user and does not interact with the LDAP server for login authentication for subsequent attempts even when there are 2 more attempts left on the LDAP server for that user.

- For an imported LDAP user, **MaxLoginAttemptsAllowed** is set to 5 in the Avaya IC system and 3 on the LDAP server.

  After 3 unsuccessful login attempts to the Avaya IC system, the LDAP server disables the login for that user. However, the Avaya IC system interacts with the LDAP server for login authentication for next 2 subsequent attempts as Avaya IC disables the login only after 5 unsuccessful attempts.

Note:

The Avaya IC system does not allow the LDAP user to log in to the Avaya IC system if the LDAP user is created with an empty password.
In Avaya IC system, there are rules of disabling and preventing subsequent login if the password entered is incorrect. You can disable this rule for LDAP users by setting **MaxLoginAttemptsAllowed** property to 0.

Replacing default certificate for the Directory server and the IC client

To enable SSL between IC client and the Directory server for the login request, you need to exchange the certificates between the Directory server and the IC client that is requesting the login.

The IC client verifies the certificate to ensure that it is communicating with the valid Directory server and creates an encrypted channel between IC client and the Directory server. After creating the encrypted channel, the IC client sends the login information to the Directory server. The Directory server authenticates the IC client based on the credentials that IC client sends.

IC provides self signed certificates out-of-box for the purpose of creating an encrypted channel between IC client and the Directory server. However, you can create and use your own certificates for the same purpose.

The Service Pack bundles Out-of-Box self signed certificates for this purpose of creating the encrypted channel between the client and Directory Server. However, customers are free to create and use their own certificates for the same.

The certificates that you can use for creating encrypted channels are classified in to the following categories:

Self signed certificates: Using CA signed certificates might result in a complicated setup in terms of host name validation. Some customers may not opt for such an arrangement, or may not require such a complicated setup. To help such situations, IC also supports self-signed certificates to be used to establish a secure SSL connection between the clients and Directory Server. In this case, the CA certificate to be used on the client side is essentially the same self-signed server certificate. When the client attempts a secure connection to the Directory Server, it tries to validate the certificate the server sends it. If the certificate is self-signed, it tries to match the certificate received from the server with the certificate which exists on the client side. If they match, then the handshake is successful, else the connection is rejected by the client.

Note: In case of a self-signed certificate, a successful certificate's FQDN validation by the client is optional during SSL handshake and Directory Server certificate may contain any information in certificate's commonName field or certificate's dNSName field of the subjectAltName.

Important: If Directory Server is using self-signed certificate then only single certificate should be deployed and configured on different Directory Server machines (Primary and Secondary). The same self-signed certificate should be distributed to all the client machines, and needs to be copied in to `IC_INSTALL_DIR\etc` folder with the name root_cert_AvayaIC_Client.pem.

Certificates signed by Certificate Authority (CA): These certificates are either signed by a well known CA e.g. VeriSign etc. or signed by a self-created CA. The signing authority verifies the existence of the business and the ownership of the Fully Qualified Domain Name (FQDN) to provide additional security. When using this option, the customers need to ensure that the FQDN on the certificate needs to match the FQDN of the Directory Server on which it is installed. As IC operates on IP addresses rather than host names, a proper reverse IP lookup mechanism needs to be setup so that the IP is resolved to the correct hostname. This can be achieved through either of the well-known mechanisms like DNS, NIS, local hosts file, and so on. The signed certificate should be installed on the machine running the Directory Server, in `IC_INSTALL_DIR\etc` folder. The certificate name can be entered in the respective server's configuration tab using IC Manager. The CA's (signing authority's) certificate, who has signed the Directory Server SSL certificate, must be distributed to all the client machines, and needs to be copied in to `IC_INSTALL_DIR\etc` folder with the name root_cert_AvayaIC_Client.pem. The name of the CA certificate cannot be changed, and has to be the one mentioned previously. You must also ensure that all the certificates are in the PEM format. During the initial handshake, the client receives the server certificate and validates its credentials using the CA certificate. If the certificate is validated successfully, then the client tries to match the FQDN of the host it is connecting to with the FQDN name in the certificate's commonName field or certificate's dNSName field of the subjectAltName. If the DNS names match, then the handshake is successful, and encrypted data is exchanged between the two nodes. If the DNS names do not match, the client rejects the connection.

IC clients support the use of wildcard characters in FQDN name in CA signed server certificate's commonName field or certificate's dNSName field of the subjectAltName. The accepted wildcard characters are described at http://support.microsoft.com/kb/258858.

Accepted wildcard examples:

- www.example.com matches www.example.com
- *.example.com matches www.example.com
- w*.example.com matches www.example.com

- ww*.example.com matches www.example.com
- Www.Example.com matches www.examPle.cOm

Non-accepted wildcard examples:

- *www.example.com
- *w.example.com
- w*w.example.com
- *ww.example.com does not match www.example.com
- www.e*ample.com does not match www.example.com
- www.*ample.com does not match www.example.com
- www.ex*.com does not match www.example.com
- www.*.com does not match www.example.com
- example.com does not match *.com does not match www.example.com
- www.example.abc.com does not match *.abc.com
- example.com does not match *.*
- example does not match *
- abc.def.example.com does not match a*.d*.example.com
- www.example.com.au does not match *.*.com.au
- www.example.com.au does not match www.*.com.au

Note:

The Directory Server fully FQDN must be present in the respective certificate's commonName field or certificate's dNSName field of the subjectAltName or both for the successful SSL handshake in case of CA signed certificate.

IC Client supports multiple commonName fields in the server certificate as well as multiple FQDN configured in the certificate's dNSName field of the subjectAltName. This means, multiple FQDN can be used in one certificate either by using multiple commonName fields in certificate or by having multiple dNSName field entry in the certificate's subjectAltName field.

Important points for CA certificates:

- If Directory Server uses CA signed certificate on different Directory Server machines, primary and secondary, then you must use only a single certificate containing multiple FQDNs of different Directory Server machines, Primary and Secondary, by entering different FQDNs in the certificate with the help of:
  - Multiple commonName field of the certificate, or
- Multiple dNSName field of the subjectAltName of the certificate, or
- Both of the previous options, or

- Using accepted wildcard characters for FQDN in the certificate.
  - In this case, the single CA's certificate must be distributed to all the client machines, and needs to be copied in to `IC_INSTALL_DIR\etc` folder with the name root_cert_AvayaIC_Client.pem.
- Multiple CAs can be used to sign certificate(s) under following circumstances:
  - Different CAs signing a single certificate at different hierarchy level and creating a certificate chain inside that certificate, or
- Different certificates (containing different FQDN information) used for different Directory Server machines (Primary and Secondary) signed by different CAs, or
- Both of the previous options
  - In this case certificates of ALL of the CAs involved in signing server certificate(s) needs to be appended one after another (not necessary in any particular order) in to root_cert_AvayaIC_Client.pem file. This file should be distributed to all the client machines and should be copied in to `IC_INSTALL_DIR\etc` folder with the same name.

    For example,

    ```
    -----BEGIN CERTIFICATE-----
    <CA 1 Certificate>
    -----END CERTIFICATE-----
    -----BEGIN CERTIFICATE-----
    <CA 2 Certificate>
    -----END CERTIFICATE-----
    -----BEGIN CERTIFICATE-----
    <CA 3 Certificate>
    -----END CERTIFICATE-----
    ..... .
    ```
  - Multiple CA certificates can be appended in to root_cert_AvayaIC_Client.pem file using notepad or any other text editing tools.

Note:
IC Active Directory/LDAP integration feature supports certificate chain depth (signing hierarchy) up to 9 levels.

Creating a self-signed server certificate

Note:
Use the same procedure to create self-signed certificates for the Windows and Unix based clients and servers.

To create a self-signed server certificate:

1. Generate pass-phrase protected private key for the Directory server.

   ```
   openssl genrsa -des3 -out domain_key_AvayaIC_Server.pem 1024
   ```

2. Create the self-signed server certificate.

   ```
   openssl req -new -x509 -extensions v3_usr -key
   domain_key_AvayaIC_Server.pem -out domain_cert_AvayaIC_Server.pem -days
   1095
   ```

3. Create a copy of the self-signed server certificate to be used as IC Client's trusted certificate:

   ```
   copy domain_cert_AvayaIC_Server.pem root_cert_AvayaIC_Client.pem
   ```

Creating a CA certificate

Perform the following procedure to create a CA certificate and then create a server certificate signed by CA.

To create a CA certificate:

1. Generate pass-phrase protected Private Key for CA:

   ```
   openssl genrsa -des3 -out root_key_AvayaIC_CA.pem 1024
   ```

2. Create the CA certificate.

   ```
   openssl req -new -x509 -extensions v3_ca -key root_key_AvayaIC_CA.pem
   -out root_cert_AvayaIC_CA.pem -days 5475
   ```

3. Generate pass-phrase protected private key for server.

   ```
   openssl genrsa -des3 -out domain_key_AvayaIC_Server.pem 1024
   ```

4. Create the server certificate request.

   ```
   openssl req -new -key domain_key_AvayaIC_Server.pem -out
   domain_req_AvayaIC_Server.pem -days 1825
   ```

5. Sign the request with the Root CA and make the Server certificate containing the Server public key.

   ```
   openssl x509 -req -days 1095 -in domain_req_AvayaIC_Server.pem
   -extensions v3_usr -CA root_cert_AvayaIC_CA.pem -CAkey
   root_key_AvayaIC_CA.pem -CAcreateserial -CAserial ca.srl -out
   domain_cert_AvayaIC_Server.pem
   ```

6. Create a copy of the CA Certificate to be used as client's trusted CA.

   ```
   copy root_cert_AvayaIC_CA.pem root_cert_AvayaIC_Client.pem
   ```

Passphrase protected server private key

Each server side certificate contains the public key along with other information, such as FQDN and has a corresponding private key, which is used for asymmetric encryption and decryption of the SSL communication. The private key can be a part of the certificate file or can reside in a different file.

The default key file that the Directory server will read at startup is the `domain_key_AvayaIC_Server.pem` file. The key file name can be changed using Directory Server configuration properties using IC Manager. If the key file is a part of the certificate, you must specify the certificate file name in the properties.

The private key could be saved on the file system as is, or in an encrypted form protected by passphrase. If the key is encrypted, then a passphrase is required by Directory Server for decoding the private key. The passphrase can be configured through IC Manager's Configuration tab for respective Directory Server.

The default certificates installed with this Service Pack will not provide SSL security due to the fact that the default server private key is shared with all the customers using this Service Pack. In order to keep the Active Directory/LDAP password secure, customers must create either a new self-signed certificate or create/get a CA signed certificate. A CA signed certificate must be used as it prevents man-in-the-middle attack through certificate's FQDN validation which is absent in self-signed certificate.

Adding secure email code in the custom website

For Interaction Center 7.3.3 and later, in the out of the box website, there is already code for SSL and SMTP authentication support in the escalate.jsp file. If you are using a custom website and you want to enable SSL and SMTP authentication support on the custom website then you must add the following code to your custom escalate.jsp file:

```
//if no mail account data has been set use the GetSysInfo methods to try and find an email server

                com.quintus.toolkit.MailAccountManager.MailAccountInfo accountInfoFromRouting = GetSysInfo.getMailAccountInfo(mailAccount);

                com.quintus.toolkit.MailAccountManager.MailAccountInfo accountInfoFromTenantID = GetSysInfo.getFirstMailAccountInfo(tenantID);


If((accountInfoFromRouting.getEmailAddress()!=null ) && (accountInfoFromRouting.getEmailAddress().length()>0)){


EmailEscalate.setMailAccountInfo(accountInfoFromRouting);
```

```
Debug.println(Debug.CRITICAL_MSG, "escalate.jsp",
session.getId(),"Mailaccount set using the RoutingHint:: [" +
accountInfoFromRouting.getEmailAddress() + "]");
                                                }else
if((accountInfoFromTenantID.getEmailAddress()!=null) &&
(accountInfoFromTenantID.getEmailAddress().length()>0)){

EmailEscalate.setMailAccountInfo(accountInfoFromTenantID);

Debug.println(Debug.CRITICAL_MSG, "escalate.jsp",
session.getId(),"Mailaccount set using the TenantID:: [" +
accountInfoFromTenantID.getEmailAddress() + "]");
```

After adding the above code, you must add the CA client certificates for the SMTP server that you are using in the default Java Trust Store which is used by ICM and Website shipped as part of the IC installation. For example:

```
"c:\Avaya\IC73\Java\bin\keytool.exe" -import -alias emailserver_smtp -file
C:\SMTPSSLsupport\smtp.emailserver.com.cer -keystore jssecacerts -storepass
<password>
```

Chapter 7: Using Content Analyzer for automated email processing

Avaya Interaction Center includes an optional component called Avaya Content Analyzer. When an email contact comes into your contact center, Content Analyzer uses natural language processing and statistical analysis on the text of the message to categorize the email contact based on a set of pre-defined topics in a content analysis Knowledge Base. The results of this analysis can be used to:

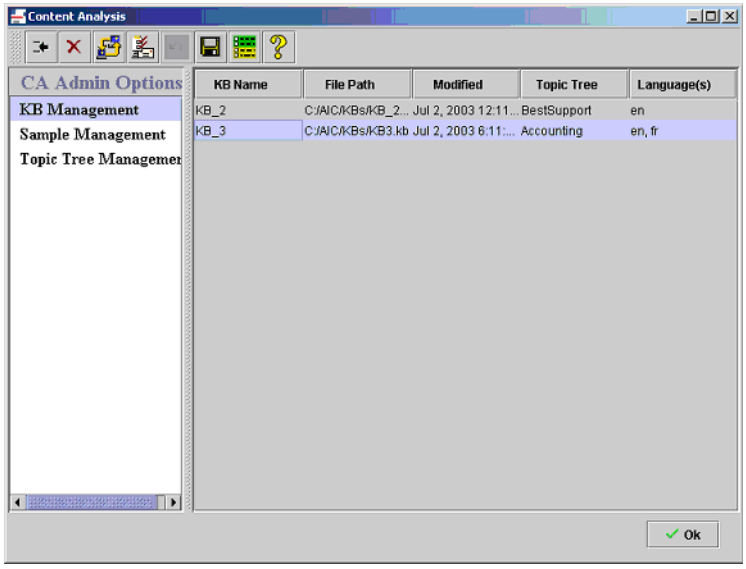
- Identify the language the email is written in so that email workflows can make more intelligent routing decisions. For example, emails written in Spanish can be sent to an agent who can read Spanish, or emails in unsupported languages can be sent to a supervisor for further investigation.
- Create an auto acknowledgement for customer emails.
- Create an intelligent automated response that can be sent back to the customer without requiring agent intervention.
- Route the email to the appropriate agent or group based on the topic of that email.
- Find a set of suggested responses in the Web Self-Service database that can be forwarded to the agent along with the original email.

Content Analyzer can identify emails written in: Chinese, English, French, German, Italian, Japanese, Korean, Portuguese, and Spanish.

Additionally, Content Analyzer can be used in conjunction with the email quality assurance process to provide screening of agent replies for suspect contents. If content analysis indicates that an outbound email might contain inappropriate content, the workflow can forward the email to a supervisor for review before it is sent to the customer. For details on creating workflows, see *Avaya Workflow Designer User Guide*.

Note:
Content Analyzer is not automatically included with Avaya IC. If you want to use this feature, you must purchase a separate license for it. For details, contact your Avaya Sales representative.

The basic Content Analyzer interface is as follows:



This section contains the following topics:

- Setting up Content Analyzer on page 171
- Designing the topic trees on page 173
- Creating topic trees on page 174
- Working with samples on page 176
- Working with Knowledge Bases on page 182
- Putting the validated Knowledge Base into production on page 189
- Maintaining your Knowledge Bases on page 190
- Maintaining your samples and sample sets on page 193

Setting up Content Analyzer

Before Content Analyzer can begin processing your company's emails, you need to:

1. Create and configure the Content Analyzer Administrative server. The Content Analyzer Administrative server must be functional before you can begin working with Knowledge Bases, and the IC Email server must be functional before you can search for new samples from existing emails in the IC Contact Center. For details, see IC Installation and Configuration and CAAdmin (Content Analyzer Administration) server on page 438.

2. Decide what topics Content Analyzer should use to categorize the emails that it processes, and how to arrange those topics in a tree structure. If you want Content Analyzer to handle several different types of tasks, you might end up with one structure for each task type. For example, you could have one structure for incoming emails and another structure for outgoing emails. These topic structures form the framework of your Knowledge Bases, so it is very important to design them carefully before you begin implementation. For details, see Designing the topic trees on page 173.
3. Open the Content Analyzer Administrator by selecting **Content Analyzer** in the Avaya IC Manager toolbar or by selecting **Tools > Content Analysis**.
4. Create and save one or more Topic Trees that reflect the structures you decided on in Step 2. For details, see Creating topic trees on page 174.
5. Collect emails, tag them with the topics created in the topic trees, and save them as samples, or sample sets, for use in training and validating content analysis Knowledge Bases. For details, see Working with samples on page 176.
6. Create one or more Knowledge Bases and associate each Knowledge Base with the appropriate Topic Tree. For details, see Creating a Knowledge Base on page 182.
7. Train the Knowledge Base using a set of samples that you have collected, tagged, and saved. For details, see Training a Knowledge Base on page 183.
8. Validate the Knowledge Base by having Content Analyzer analyze a selected sample set to evaluate the effectiveness of the trained Knowledge Base. For details, see Validating a Knowledge Base on page 185.
9. Put the validated Knowledge Base into production. For details, see Putting the validated Knowledge Base into production on page 189.

Customizing the display of warning messages

The warning dialog boxes in Content Analyzer have a check box at the bottom called **Show This Dialog Again?** that facilitates in suppressing subsequent appearances of that dialog box. You can either use this check box to suppress the warnings individually, or you can use **User Options** to suppress (or re-enable) all of the warnings at once.

Note:
Content Analyzer remembers your settings for each warning dialog box across sessions on an individual machine, so each time you log in to any machine you have used before, Content Analyzer will display or suppress those warnings based on your previous selections on that machine.

To suppress warning messages:

1. Select **User Options** on the Content Analyzer toolbar.
2. In the **User Options** dialog, select either **Enable All Warnings** or **Disable All Warnings**.
3. Select **OK**.

Designing the topic trees

Every Content Analyzer Knowledge Base has an associated topic tree that forms the underlying structure of the Knowledge Base. There is one topic at the top (the root node) that provides the name of the tree and one or more levels of general topics below that (the branch nodes). The topics at the end of each branch (the leaf node) should be the most specific topics in that path.

If your contact center works with emails written in more than one language, You must have the second level branch nodes in your tree as language nodes. You should define one language node for each language you want to use, and then create the appropriate topics under each language. For details about multi-language support in Content Analyzer, contact your Avaya Technical Support representative.

After you have created your topic nodes, you collect samples and assign them to those nodes. Content Analyzer uses those samples to build analysis rules so that it can analyze email texts and classify them according to the topics in your Knowledge Base. This analysis results in a list of the topics that the email matches, along with a confidence score for each match. Content Analyzer sends the list of matches and confidence scores back to the workflow, where they can be used to make routing decisions, generate auto-responses, or flag the email for further review by a supervisor.

Along with the associated topics, each node can also have a set of associated keywords. If your company uses the Web Self-Service feature of Avaya ICs Web Management, you can use these keywords to map the topics in your Knowledge Bases to the documents in your Web Self-Service database. After a workflow sends an email to Content Analyzer for processing, the workflow can retrieve the topic pathname and keywords associated with any matched topics. It then uses that information to search the Web Self-Service database for matching documents. These documents can then be delivered to the processing agent as suggested responses along with the email.

For more information on:

- Setting up a Web Self-Service database, see Setting up the Web Self-Service feature on page 320.
- Creating a workflow, see *Avaya Workflow Designer User Guide*.

For Content Analyzer to make useful classification decisions, the topic tree must be as robust and logically structured as possible. Before you create the actual topic tree, make sure you know what topics you need and how the topics should be related. If you create a small number of topics, then emails may get lumped together even when they are very different. If you create a large number of topics, then Content Analyzer may return a list of possible matches that is too long to be easily processed.

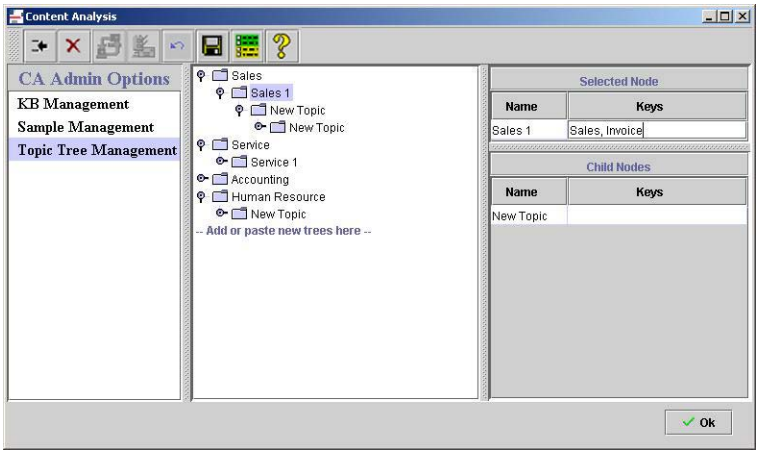
Creating topic trees is an iterative process. After you have created one and trained its associated Knowledge Base, you need to test the system thoroughly to make sure Content Analyzer produces the results that you expect. If it does not, or if your business model changes and Content Analyzer no longer produces the results you need, then you need to go back and evaluate both your samples and your topic trees. For more information on creating a topic tree, see Creating topic trees on page 174. For more information about tuning an already-existing Knowledge Base, see Maintaining your Knowledge Bases on page 190.

Creating topic trees

To create a topic tree:

1. Open the Content Analyzer Administrator by selecting **Content Analyzer** in the Avaya IC Manager toolbar.
2. In the left pane, select **Topic Tree Management**. The right pane is divided into two vertical sections, with one showing the structure of all the topic trees you have defined and the other showing details about the selected node and its children.

   See the following figure:



3. Select **Add Tree** in the toolbar or right-click in the section labelled **Add or Paste New Trees Here** and select **Add New Tree** from the pop-up menu. Content Analyzer displays the **Add Tree** dialog box.
4. Enter the name for this tree. Click **OK**.
5. If this is going to be a multi-language tree, right-click the root node and select **Add Language**. In the **Name** field of the **Selected Node** section, select the required language from the drop-down list.

   Repeat this step for each language node you want to add.
6. Create lower-level topic nodes by right-clicking on the node under which you want to add the new topic and selecting **Add Topic** from the pop-up menu. Content Analyzer adds a new topic called `New Topic`. You can change the name using the **Name** field in the **Selected Node** section. (Topic names are for identification purposes only. They do not affect the way Content Analyzer matches emails to topics.)

   Repeat this step for each topic you want to add.
7. Select **Save** to save your changes.

Note:
Content Analyzer saves all topic trees, not just the current one.

For more information, see Working with topics.

Working with topics

After adding a topic, you can:

Change its name: Select the topic and then click in the **Name** field in the **Selected Node** section. Enter the new name and press **Enter**.

Add keywords: Keywords map the topic to the documents in your Web Self-Service database. To add them, select the node and then click in the **Keys** field in the **Selected Node** section. To add multiple keywords, separate them with a semi-colon. Keywords cannot contain spaces, commas, or periods.

Tip:
If you do not have a specialized language keyboard, you can enter accented characters by holding the **ALT** key while typing the standard four digit code for that character on your numeric keypad. For a complete list of character codes, see Appendix D: Typing special characters on page 566.

You can enter Japanese, Korean, and Chinese characters in a localized Windows environment using the Windows Input Method Editor (IME).

Note:
The `AnalyzeCA` workflow uses the keywords to search the Web Self-Service database for documents that can serve as suggested responses. Make sure that both you and your workflow designer agree on what keywords to use.

Copying, moving, and deleting topics

You can copy, move, or delete nodes and subtrees. For details about what happens when you perform these operations on nodes that have associated samples, see Updating topic trees on page 190. To:

Copy a single node: Right-click the node that you want to copy and select **Copy Node**. Then right-click the node under which you want the copy to appear and select **Paste**.

Copy or move a node and all its children to another location: Right-click the top-most node and select **Copy Subtree** or **Cut Subtree**. To specify that the selected nodes should be copied or moved:

- Under a node in an existing tree, right-click that node and select **Paste**.
- In a new tree, right-click in the area labelled **Add or Paste New Trees Here** and select **Paste New Tree**.

Note:
If the subtree that you are copying or moving begins with a language node, then you must paste it under the root node of an existing tree. If you copy or move an entire tree that contains language nodes, then you must paste it into the area labelled **Add or Paste New Trees Here** to create a new tree. You cannot add language nodes under anything other than a root node.

Tip:
If you want to duplicate the same topic structure under multiple language nodes, create the topic structure once under one language node, then right-click that language node, select **Copy Subtree**, and paste it under the root node. Select the language node in the pasted subtree and choose a new appropriate language in the Selected Node table for the newly-copied subtree.

Delete the topic and all its children: Right-click the topic and select **Delete Subtree** from the pop-up menu. Content Analyzer changes all of the affected topic names to red and puts the note '[deleted]' after them. Content Analyzer does not actually remove the deleted topics until you save the tree. Until that time, you can restore any deleted nodes.

To restore previously deleted nodes, right-click the parent of the deleted topic nodes and select **Undelete Subtree** from the right-click menu. Content Analyzer undeletes the node and all the nodes under it, then checks the node's parent. If the parent is marked as deleted, Content Analyzer restores that node as well. It continues working up the tree until there is a path of undeleted nodes from the root to the first node you restored.

Assigning samples to topics

After setting up your topic nodes, you need to assign samples to each node so that Content Analyzer can build the analysis rules that allow it to match incoming emails to the topics in your tree. For details, see Working with samples on page 176 and Training a Knowledge Base on page 183.

Tip:
If there are unsaved changes in a topic tree and you wish to cancel those changes, right-click on the tree's root node and select **Restore Tree**. Content Analyzer restores the selected topic tree to the last version saved in the database.

Working with samples

A topic tree provides the structure, or skeleton, of your Knowledge Base. By itself, it does not provide Content Analyzer with enough information to process a new email message. The intelligence of your Knowledge Base comes from the samples that you associate with each topic in your tree.

When Content Analyzer analyzes an email, it performs the analysis using the rules it generates from the text samples you associate with the Knowledge Base during the training process. This analysis determines whether the text matches any topic or topics in the Knowledge Base's topic tree.

If your samples are clearly defined and properly associated with their topics, then Content Analyzer can make extremely accurate matches. If your samples contain overlapping topics or do not really match the topic that they are associated with, then Content Analyzer will probably produce unsatisfactory results.

Therefore, you must compile, organize, and tag your samples as carefully as possible.

To create samples for Content Analyzer:

1. If you want to use emails that are not already stored in your Avaya IC database, import them into the `qem_message` table in the ccq database. For details about importing messages from previous versions of Avaya IC, see *IC/OA Software Upgrade and Data Migration*. If you need further assistance, contact your Avaya Technical Support representative.
2. If you want to create some samples by hand, see Creating individual samples on page 181.
3. Search, using various search criteria, existing emails in the IC database and select from the search results a representative group of samples and associate them with topics from a topic tree created earlier, then combine those samples into sample sets. For details, see Tagging samples and creating sample sets on page 177.
4. Train your Knowledge Base so that it builds proper analysis rules based on the samples you have associated with each topic. For details, see Training a Knowledge Base on page 183.
5. Use a sample set to validate the accuracy of your Knowledge Base. For details, see Validating a Knowledge Base on page 185.
6. Periodically add new samples so that you can re-tune your Knowledge Base with updated information. For details, see Maintaining your Knowledge Bases on page 190.

Tagging samples and creating sample sets

After collecting emails to use for your samples, you need to tag each sample with the topics it is associated with. After you have tagged the samples, you can create sample sets that you can use to train and validate the Knowledge Base so that Content Analyzer can begin processing new emails.

A sample set is a named collection of samples that can be used to train and validate a Knowledge Base. The samples themselves can belong to any number of sample sets. After you create a sample set, you can delete that set, but you cannot change the samples that are in that set. If you delete a set, Content Analyzer removes the associations between the samples in the set and the set itself. Content Analyzer does not delete the actual samples themselves.

Tip:
If you cannot find an appropriate sample for a given topic, you can create those samples by hand. For details, see Creating individual samples on page 181.

Because you cannot add or delete samples from an existing sample set, you may want to create a series of small sample sets and then combine them together to form increasingly larger sets until you have created your ideal training sample set. For details, see Creating new sample sets from existing sets on page 193.

When you tag your samples, you must do the following:

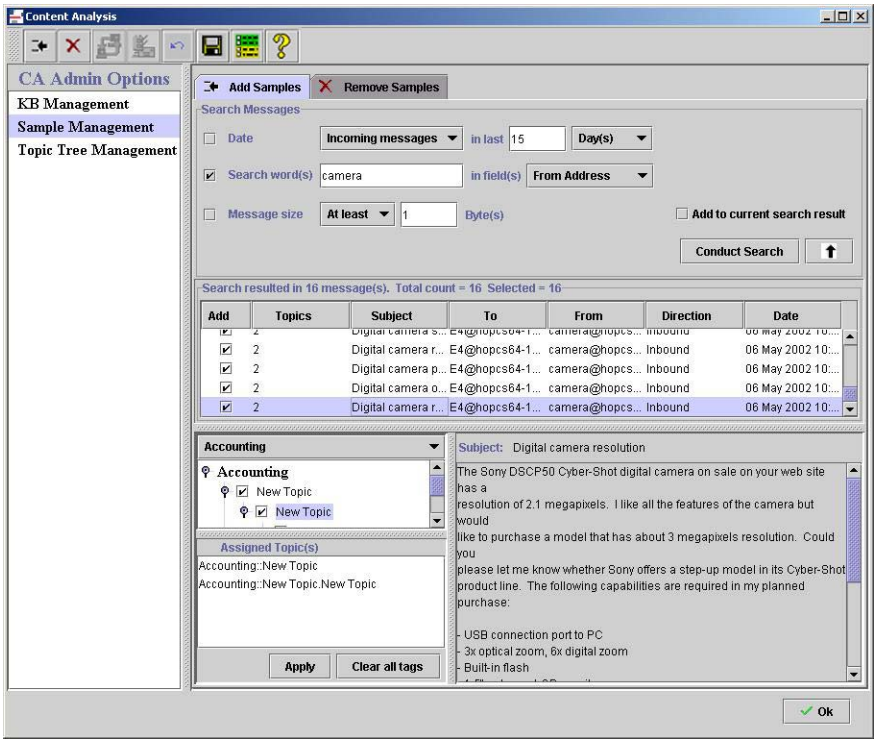
- If a node has only one child, both the parent and the child node *must* have associated samples. The associated samples can be the same samples.
- If a node has more than one child, at least two of the child nodes *must* have associated samples.
- Every topic in the tree should have at least 30 to 40 samples associated with it. Samples can be tagged to multiple topics if they apply to both child and parent nodes.

Creating a list of samples

To create a list of samples:

1. Open the Content Analyzer Administrator and select **Sample Management** in the left pane.

   Content Analyzer displays the Add Samples tab, as shown below:



2. On the **Add Samples** tab, use the **Search Samples** section to find the emails you want to look at from those already in the Avaya IC database. You can restrict messages by:

- Incoming or outgoing by selecting the **Date** check box and then selecting the appropriate choice from the drop-down list. To view both types of messages, select **Both** in this field. If you select **Incoming**, Content Analyzer searches for regular incoming email and any replies from a customer. If you select **Outgoing**, Content Analyzer searches for agent replies to a customer.
- Date by selecting the **Date** check box. You can limit the list to incoming or outgoing messages within the last *n* number of days, months, or years. When Content Analyzer determines the value for *n*, Content Analyzer takes the last full unit starting at the previous midnight and adds the current time. For example, if you specify the minimum search time **1 day** at 3:00 PM on a Thursday, Content Analyzer includes time span from 12:00 AM Wednesday to 12:00 AM Thursday, plus the time from 12:00 AM Thursday to the current time of 3:00 PM Thursday, for a total of 39 hours.
- Search words by selecting the **Search words** check box. If you select this option, you can enter a comma-delimited list of search terms in the associated text field, and then specify whether the terms can appear in the subject, body, subject and body, To address, or From address.

  Content Analyzer performs a case-insensitive AND search for all of the search terms you enter in this field. If you enter a phrase, such as “home computing”, as one of your search terms, then that exact phrase must appear in the email for it to be a match. Content Analyzer will match substrings; for example, “book” would match “Book”, “notebook”, “bookbag”.

  If you want to specify that there must be some text in the selected fields but you do not care what the text actually is, enter an asterisk (*) in the Search words field. You cannot use any other wildcards in this field or specify a logical NOT or OR search.
- Message size by selecting the **Message size** check box. If you select this option, you can specify whether the message should be at least or at most the number of bytes specified in the bytes field.

3. When you have finished adding your search criteria, select **Conduct Search**. Content Analyzer may display one or more progress bars showing the status of the search.

   Tip:
   While the search is progressing, you can begin associating topics with emails as soon as they are displayed in the Search Results list. For details, see Associating topics and creating sample sets on page 180.

   Because you cannot add samples to an existing set, all the samples you want grouped into the set must be displayed in the **Search Results** list. If you want to add more samples to the search list, adjust your search criteria, select the **Add to current search results** check box, then select **Conduct Search** again. (If you do not select the **Add to current search results** check box, then Content Analyzer replaces the contents of the **Search Results** list with the results of the new search.)

4. When you are satisfied with your search list, you can select the **Up Arrow** to collapse the **Search Messages** section so that you can view the maximum number of search results at a time.

Associating topics and creating sample sets

To associate a sample with one or more topics and create the sample set:

1. Select the sample in the **Search Results** list. Content Analyzer displays the subject and body of the sample in the preview area below the **Search Results** list.

   Tip:
   After selecting a sample, you can select all contiguous samples between that sample and a second sample by clicking on the first sample and **Shift+clicking** on the second sample. In addition, you can include non-contiguous samples by **Control+clicking** on those samples.

2. In the area below the **Search Results** list, select the appropriate topic tree from the **Select Tree** drop-down list. Content Analyzer displays a list of all the topics in that tree. All of the samples that you want to use to train a particular Knowledge Base *must* be tagged to the topic tree that is associated with the Knowledge Base. In other words, the samples must belong to the topic tree that you selected when you created the Knowledge Base).

   Note:
   When you assign samples to a topic, make sure that:

   – At least two of those samples are unique to that topic and not assigned to any other topic in the tree.

     - and -

   – There are at least 2 unique samples assigned to its sibling topics.

   If all of the samples assigned to a particular topic are shared with other topics, Content Analyzer may not successfully train that topic because it might not be able to distinguish between that topic and the ones with which it shares samples.

3. Select the relevant topics and select **Apply**. Content Analyzer associates the selected topics with the sample, or samples, you selected in the **Search Results** list.

   Repeat this step until all relevant topics have been associated with the selected samples.

4. For each sample that you want to add to the sample set, make sure that the check box in the **Add** column is selected. Content Analyzer automatically checks the **Add** box when you associate a sample with a topic.

   Tip:
   The **Topic** column shows the number of topics with which the given sample is associated. All of the samples that you intend to put into a sample set must be associated with at least one topic from the same topic tree.

5. When you are done, select **Save** in the toolbar. If the samples you selected are associated with topics from multiple topic trees, Content Analyzer saves them as individual samples. If they are associated with topics from the same topic tree, Content Analyzer displays a dialog box that presents options to save the samples as a sample set or to keep them as individual samples. To save them as a sample set, select **Sample Set**, enter a name for the new sample set, then select **Save**.

   Tip:
   If you want to use the same sample (or samples) in a sample set associated with two different trees, you need to do that in two steps: First, associate the samples you want to use with the first tree and select **Save**, then save the samples as a sample set at the prompt. Second, repeat this procedure for the second tree, associating whatever samples are associated with the first tree to topics in the second tree. Content Analyzer creates two sample sets with overlapping samples.

After you have tagged your samples, you can create and train your Knowledge Base. For details, see Working with Knowledge Bases on page 182.

Creating individual samples

If you cannot find a sample that you want to associate with a particular topic, you can create it manually. If you are going to use Content Analyzer to check outbound emails, this is a good way to add samples that can be used to identify emails with inappropriate language or proprietary company information.

To create a new sample:

1. Open the Content Analyzer Administrator, select **Sample Management** in the left pane, and go to the **Add Samples** tab.
2. Select **Create New Sample** in the toolbar. Content Analyzer moves the focus to the preview area on the **Add Samples** tab and turns on Edit mode.
3. Enter the subject and body text for this sample.

   If you do not have a specialized language keyboard, you can enter accented characters by holding the **ALT** key while typing the standard four digit code for that character on your numeric keypad. For a complete list of character codes, see Appendix D: Typing special characters on page 566.

   You can enter Japanese, Korean, and Chinese characters in a localized Windows environment using the Windows IME (Input Method Editor). If you want to enter characters of these Eastern Asian languages in English Windows environment, you must install these languages and enable the language-specific input service from **Regional and Language Options** in the Windows **Control Panel**.
4. Specify whether this sample applies to inbound or outbound emails.
5. Select the topics that you want to associate with this sample.
6. Select **Save**. Content Analyzer adds the sample to the **Search Results** window.

7. To save the sample to the database, select **Save** in the toolbar.

Working with Knowledge Bases

After you have created your topic trees and organized your samples into sample sets, you can create a Knowledge Base that Content Analyzer will use to evaluate new emails in a production environment. To do so:

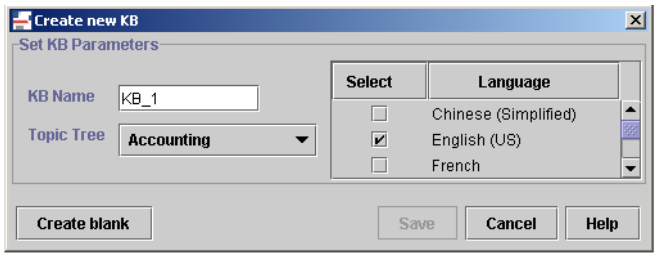
1. Create one or more Knowledge Bases and associate each of them with the appropriate Topic Tree. For details, see Creating a Knowledge Base on page 182.
2. Train the Knowledge Base using a set of samples that you have collected, tagged, and saved. For details, see Training a Knowledge Base on page 183.
3. Validate the Knowledge Base by having Content Analyzer analyze a selected sample set to evaluate the effectiveness of the trained Knowledge Base. For details, see Validating a Knowledge Base on page 185.
4. Put the validated Knowledge Base into production. For details, see Putting the validated Knowledge Base into production on page 189.

Creating a Knowledge Base

To create a Knowledge Base:

1. Open the Content Analyzer Administrator and select **KB Management** in the left pane.
2. Select **New** in the toolbar. Content Analyzer displays the **Create New KB** dialog box.

   See the following figure:



3. Enter a descriptive name for the Knowledge Base.
4. Select the topic tree for the Knowledge Base from the drop-down list. (For details, see Creating topic trees on page 174.)
5. If the selected topic tree includes language nodes, then the Knowledge Base will automatically use those languages. Otherwise, select the languages that will be associated with this Knowledge Base.

CAUTION:
If you do not select a language, Content Analyzer configures the Knowledge Base to use all of the languages that Content Analyzer supports. This can consume a significant amount of resources on all of the machines on which the Content Analyzer servers run.

6. Select **Create blank**. Content Analyzer displays a message confirming that the Knowledge Base has been successfully created.
7. Save the Knowledge Base by selecting **Save** in the toolbar and entering a fully-qualified name for the Knowledge Base. The specified path must be accessible from the machine on which the Content Analyzer Administration server is running. (For example, if you specify a mapped drive, that drive must be mapped on the machine hosting the Content Analyzer Administrative server as well.)

Once you have a blank Knowledge Base, you need to train it. For details, see Training a Knowledge Base on page 183.

Training a Knowledge Base

After you have tagged your samples and created a sample set, you can use that sample set for new or incremental Knowledge Base training. If you have an untrained Knowledge Base or you want to remove any previous training from a previously-trained Knowledge Base, use new training. If you want to add to the training that has already been done on an existing Knowledge Base, use incremental training.

When you train a Knowledge Base, Content Analyzer goes through all of the samples in the selected sample set and develops the analysis rules that it will use when processing a new email. When it is finished, it displays the results in the **Training Results** dialog box.

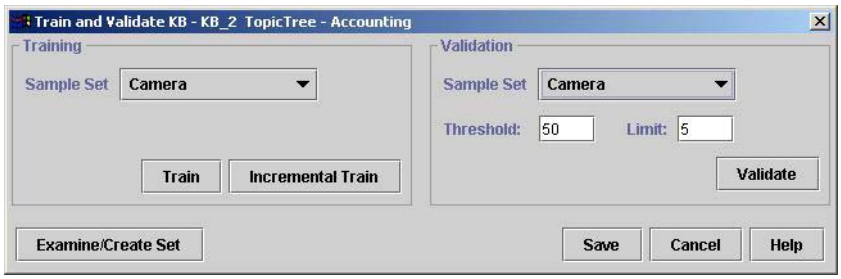
You can use the training results to make sure that each topic in your Knowledge Base was trained with a reasonable number of samples. If the distribution is proper, you can proceed to the validation step, as described in Validating a Knowledge Base on page 185.

To train a Knowledge Base:

1. Select **KB Management** in the left pane, then select the Knowledge Base that you want to train in the list shown in the right pane.

2. Select **Train/Validate** in the toolbar. Content Analyzer displays the **Train and Validate KB** dialog box.

   See the following figure:



3. In the **Training** section, select the sample set you want to use from the **Sample Set** drop-down. If you want to view or change the contents of this sample set, see Creating new sample sets from existing sets on page 193.

Note:
Make sure that the sample set you select has enough uniquely-assigned samples so that Content Analyzer can train the Knowledge Base correctly. For details, see Associating topics and creating sample sets on page 180.

4. To train the Knowledge Base for the first time or to remove any previous training information and start over again, select **Train**. To use additional samples to update a previously-trained Knowledge Base, select **Incremental Train**.

Tip:
You must select **Train** for the initial training of a Knowledge Base. Although you can do the initial training using **Incremental Train**, that option generally requires more samples during the initial training to achieve the same level of accuracy as **Train**. Incremental training is intended to refine the training of a previously trained Knowledge Base only.

Content Analyzer displays a message window stating that training is in process along with a training progress bar.

Note:
If you cancel incremental training, Content Analyzer does *not* return the Knowledge Base to its previous condition. Instead, the Knowledge Base will be partially re-trained.

When the training is finished, Content Analyzer displays the results in the **Training Results** dialog box. For information on interpreting these results, see Interpreting training results on page 184.

Interpreting training results

The training results begin with a summary section at the top of the file. This section includes the:

- Name of the sample set being processed.

- Time and date when processing began.
- Status of the training. The most common statuses are:
  - SUCCESS - Training succeeded without any problems.
  - WARNING - Training succeeded but there were rejected samples. This could be because a sample in the sample set was not associated with any topics in the Knowledge Base, or because the Content Analyzer administrative server returned a warning message during training. If you encounter this message, make sure that the Knowledge Base is synchronized with its associated topic tree. It is possible that some samples are tagged with topics that no longer exist in the Knowledge Base.
  - SERVER FAILURE - The Content Analyzer administrative server went down or became otherwise inaccessible during the training.
- Number of samples processed.
- Number of topics trained.
- Time spent training the Knowledge Base.
- Average time spent per message.
- The number of samples accepted and rejected by the training process.

This summary section is followed by a list of the topics in the topic tree and the number of emails assigned to each topic during this training session.

First, verify that the number of samples used during the training matches the number of samples contained in the sample set. If Content Analyzer rejected a large number of samples, you need to examine your sample set carefully to determine why.

If there are obvious places where additional samples are needed, you should add those samples using incremental training, as discussed in Training a Knowledge Base on page 183. If not, you can gather more information about the Knowledge Base by validating it. For details, see Validating a Knowledge Base on page 185.

Tip:
If you want to save the results for future reference, select Save Results and specify a path and filename. This path is relative to the machine running Avaya IC Manager. Content Analyzer saves the training results to the specified path and file name.

Validating a Knowledge Base

When you validate a Knowledge Base, Content Analyzer takes the samples in the specified sample set and processes the samples as if the samples were a set of incoming emails. It compares its results to the “correct” answers you provided when you associated the samples with the topics in the topic tree. This comparison produces a set of Precision and Recall scores that you can use to verify the accuracy of your Knowledge Base. For details on how to interpret these scores, see Interpreting validation results on page 187.

Precision is the percentage of all emails identified by Content Analyzer as being in a category that actually belong to this topic, that is, the number of texts correctly matched to a topic divided by the total number of texts returned as matches for this topic.

Recall is the percentage of texts that actually belong to the category and are recognized as such by Content Analyzer, that is, the number of texts correctly matched to a topic divided by the total number of texts that should have been matched to this topic.

Before you validate your Knowledge Base, you should decide what Precision and Recall scores you consider acceptable for this Knowledge Base. For example, if this Knowledge Base is going to be used for an auto-response system, you might require a high Precision score. This information makes you confident that when Content Analyzer returns a topic, that topic has a very high probability of answering the customer's question.

On the other hand, if this Knowledge Base is going to be sending its responses to a human agent for review, you might be able to accept a lower Precision score but want a higher Recall score so that you increase the odds of the agent receiving the correct response even if the agent has to eliminate the incorrect responses manually.

After deciding what balance you want between Precision and Recall, you can validate your Knowledge Base using various threshold and limit parameters to see what results you can expect in a production environment. Each time you validate your Knowledge Base, you can change the Knowledge Base's threshold and limit parameters, and then examine the resulting Precision and Recall scores.

If you get satisfactory validation scores, you can associate the Knowledge Base with an operational CAServer. (For details, see CA (Content Analyzer) server on page 440.)

If you do not get satisfactory validation scores, it may be necessary to retrain the Knowledge Base. For details on the scores, see Using the precision and recall scores to verify the accuracy of the Knowledge Base on page 188.

To validate a Knowledge Base:

1. Select **KB Management** in the left pane, then select the Knowledge Base that you want to validate in the list shown in the right pane.
2. Select **Train/Validate** in the toolbar. Content Analyzer displays the **Train and Validate KB** dialog box.
3. In the **Validation** section, select the sample set you want to use from the **Sample Set** drop-down. This sample set must be associated with the same topic tree that is associated with the Knowledge Base. If you want to view or change the contents of this sample set, see Creating new sample sets from existing sets on page 193.
4. In the **Threshold** field, specify the minimum score (confidence level) for text-to-topic matches that must be met before Content Analyzer considers the email a match for a given topic the value can be between 0 and 100.

   Avaya recommends that you start with the default value of 50 and then change it incrementally to determine the threshold that yields the best Precision and Recall scores for your needs.

Tip:
Start with a large increment, like 10, and then switch to a smaller increment as you narrow the threshold range that produces the best scores.

5. In the **Limit** field, specify the maximum number of text-to-topic matches that Content Analyzer will return for any given email. This parameter affects the Precision and Recall scores for your Knowledge Base, although its impact is probably less than that of the threshold setting.
6. Select **Validate**. Content Analyzer processes the samples in the sample set and displays the results in the **Validation Results** dialog box. For information on interpreting these results, see Interpreting validation results on page 187.

Interpreting validation results

The validation results begin with a summary section at the top of the file. This section includes the:

- Name of the sample set being processed.
- Time and date when processing began.
- Match Count Limit set when the Knowledge Base was validated.
- Minimum Match Threshold set when the Knowledge Base was validated.
- Validation status.
- Number of samples processed.
- Number of topics validated.
- Time spent validating the Knowledge Base.
- Average time spent per message.

This summary section is followed by a list of the topics in the topic tree. For each topic, Content Analyzer shows the number of samples used for validating the topic, the Precision score, and the Recall score.

The topic list is followed by a summary of the overall Precision and Recall scores. This summary includes:

- Micro-average Precision - the average precision score across all samples used during validation.
- Micro-average Recall - the average recall score across all samples used during validation.
- Macro-average Precision - the average precision score across all topics in the tree.
- Macro-average Recall - the average recall score across all topics in the tree.

Using the precision and recall scores to verify the accuracy of the Knowledge Base

The Precision and Recall scores help you judge the accuracy of your Knowledge Base. These two scores have an inverse relationship to each other, and they are both affected by the threshold and limit settings you selected when you validated the Knowledge Base. If this Knowledge Base is going to be used for typical email processing tasks, the goal is to have both of these numbers be as close to 1.0, and as close to each other, as possible. If this Knowledge Base is for a specialized purpose (such as sending auto-responses or evaluating outbound emails), you might want the Precision scores for the relevant topics to be very high to ensure that matches to those topics are more likely to be correct.

To evaluate the accuracy of your Knowledge Base:

1. Look at the precision and recall statistics for each topic. If the scores for all topics are uniformly low, then there might be a design issue and you must:
   a. Verify that the topic structure accurately reflects the types of emails your company receives. If a few of the topics are low, then consider whether they should be combined with other topics in the tree.
   b. Make sure that the samples that you associated with each topic are truly representative of the topic. You might need to add or delete samples from each topic to improve the analysis rules Content Analyzer builds when you train the Knowledge Base.
   c. Retrain and re-validate the Knowledge Base using either new or incremental training and examine the precision and recall scores again. (For details, see Training a Knowledge Base on page 183.)

   Repeat this step until all topics have an acceptable precision and recall score.
2. When the topic scores are uniform, look at the micro and macro scores in the summary section. If these scores do not meet the goal for this particular Knowledge Base, run the validation program again, specifying a new threshold and limit value. (For details, see Validating a Knowledge Base on page 185.)

   Examine the new micro and macro scores, and re-validate again with different threshold and limit scores if necessary.

   Repeat this step until you get acceptable micro and macro scores.
3. When all of the precision and recall scores are at an acceptable level, make note of the Minimum Match Threshold value. You will need that value when you begin using the Knowledge Base to process incoming emails. (For details, see Putting the validated Knowledge Base into production on page 189.)

Tip:
You can save the last set of validation results for future reference by selecting Save Results in the Validation Results dialog box.

Putting the validated Knowledge Base into production

After you are satisfied with the results of the validation, you can put the validated Knowledge Base into production. To do so:

1. Save the Knowledge Base by selecting **Save** in the toolbar and entering a fully-qualified name for the Knowledge Base. The specified path must be accessible from the machine or machines on which the Content Analyzer Administration server and the operational CAServer are running. For details, see CAAdmin (Content Analyzer Administration) server on page 438 and CA (Content Analyzer) server on page 440.
2. If this Knowledge Base is not associated with an operational CAServer, create a new CAServer and specify the Knowledge Base name, the fully-qualified Knowledge Base file location, the minimum matching threshold, and the language for the Knowledge Base.

   If the Knowledge Base is already associated with an operational CAServer, you will see a series of warnings to stop and then restart that server so that it will use the updated Knowledge Base. For details about how to do this, see Starting or stopping a server on page 78.
3. Modify the email workflows, `AnalyzeCA` and `OutboundCA`, to use this Knowledge Base.

   In the `AnalyzeCA` workflow, you need to:

   - Specify the name of the operational CAServer in the Content Analysis `GetLanguage` workflow block
   - Specify the name of the operational CAServer and the Knowledge Base name in the Content Analysis `GetMatchedCategory` workflow block
   - Specify the minimum score (confidence level) for each match returned by Content Analyzer
   - Specify the maximum number of text-to-topic matches that Content Analyzer will return for any given email

   In the Content Analysis `QACategory` workflow block of the `OutboundCA` workflow, you need to specify:

   - The name of the operational CAServer.
   - The name of the Knowledge Base.
   - The path name of Category (topic) to match for.
   - The minimum score for the match.

   For details about these workflows, see *Avaya IC Media Workflow Reference*.
4. If you want to use the results returned by Content Analyzer to search the Web Self- Service database for suggested responses, make sure that:

   - You have included keywords with the topics of the topic tree associated with the Knowledge Base.
   - The documents that you want to use as suggested responses in the Web Self-Service database include these keywords, preferably in the language specific **Document Title** field.

- The `GetSuggestedResponse` workflow block in the `AnalyzeCA` workflow specifies that the workflow should use topic keywords in the search.

For details about the `AnalyzeCA` workflow, see *Avaya IC Media Workflow Reference*.

5. Periodically, you should validate your Knowledge Base with a set of current emails to make sure the topics are still relevant. For details, see Maintaining your Knowledge Bases on page 190.

Maintaining your Knowledge Bases

After you have initially trained your Knowledge Bases, you can begin using Content Analyzer. As time goes on, however, you should retrain your Knowledge Bases to adjust for changes to the topics that occur in the emails your contact center receives.

To maintain a Knowledge Base:

1. Create a sample set periodically from recent emails received at your contact center. (For details, see Tagging samples and creating sample sets on page 177.)
2. Use that sample set to validate the Knowledge Base and examine the results. (For details, see Validating a Knowledge Base on page 185.)
3. Use the sample set you created to incrementally train the Knowledge Base, and then create a new sample set if the validation scores are too low and run the validation procedure again. For details, see Training a Knowledge Base on page 183.
4. Continue creating new sample sets and incrementally training the Knowledge Base until the validation scores have returned to an acceptable level. If retraining is not enough, you may need to update the underlying topic tree to match the changes in your contact center. For details, see Updating topic trees on page 190.

Updating topic trees

Sometimes just retraining the Knowledge Base is not enough, and you need to update the underlying topic tree as the topics your contact center handles change. You may have to add new topics, restructure current topics, or delete old topics.

Tip:
If there are unsaved changes in a topic tree and you wish to cancel those changes, right click on the tree's root node and select **Restore Tree**. Content Analyzer restores the selected topic tree to the last version saved in the database.

When you copy, move, or delete nodes that have samples already associated with them, the following processing takes place:

Note:
All of these actions can be undone until you save the topic trees.

- If you paste nodes from one part of a tree into another part of the same tree, Content Analyzer copies the nodes and gives you the option of copying the sample associations as well. If you select this option, Content Analyzer takes each sample that was associated with the original nodes and tags those samples with the newly-copied nodes as well. Content Analyzer does not change the contents of any sample sets. In other words, the samples remain in their sample sets, but some of them are now tagged with additional topics.
- If you paste nodes across trees, you can specify two options:
  - **Maintain sample associations?** Select this option if you want the samples from the old tree to be tagged with the new nodes as well. If you select this option, Content Analyzer creates the new tags when you save the topic trees.
  - **Copy sample sets?** Select this option if you want Content Analyzer to create the same sample set structure in the new tree that exists in the source tree. Samples in the source tree's sample sets are copied to the corresponding sets for the new tree if those samples are associated with at least one topic in the new tree.

    Content Analyzer derives the names of the new sample sets from the names of the old ones. For example, if the source sample set is called `Camping`, Content Analyzer will name the new sample set `Camping(2)`.

Note:
This option applies to all nodes pasted into the topic tree regardless of where they came from. When you save the tree, Content Analyzer looks at the last setting for this option and either copies the sample sets from all newly-pasted nodes or from none of them. If you want to copy the sample sets from some trees but not others, you need to paste in the nodes in two stages: First, paste in the nodes whose sample sets you want to copy and select the **Copy Sample Sets** option. When you are done, save the trees and let Content Analyzer recreate the sample sets. Then paste in the nodes whose sample sets you do not want to copy, clearing the **Copy Sample Sets** option. When you are done, save the trees. Content Analyzer does not copy the sample sets for the second set of nodes.

- If you cut or delete nodes, then Content Analyzer removes any sample associations from those nodes. If a sample is no longer associated with any topics left in a particular tree, then Content Analyzer removes that sample from any sample sets associated with that tree. If the sample is no longer associated with *any* topics in *any* tree, then Content Analyzer removes the sample from all sample sets associated with the trees *and* from the sample database. This includes individually created samples. If you have created a sample manually, make sure that the sample is still tagged to a topic before you save your topic trees. Otherwise, Content Analyzer will permanently delete the sample.

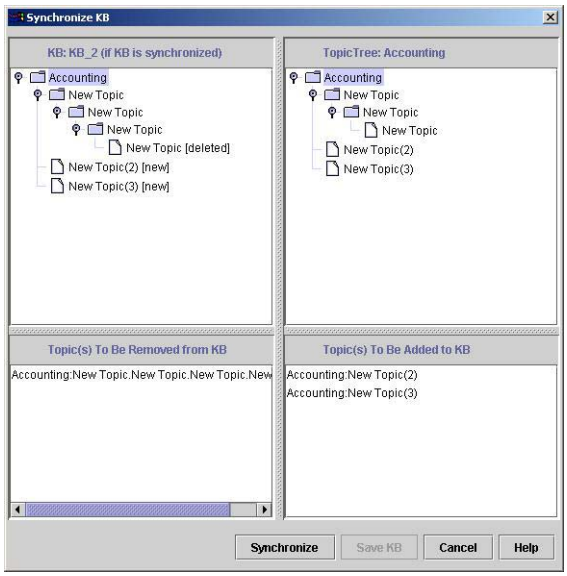
When you have finished updating your topic tree, you need to synchronize the changed tree with its associated Knowledge Base. For details, see Synchronizing a Knowledge Base on page 192.

Synchronizing a Knowledge Base

If you have updated a topic tree, you need to communicate those changes to the associated Knowledge Base. To do so:

1. Select **KB Management** in the left pane, then select the Knowledge Base that you want to synchronize in the list shown in the right pane.
2. Select the **Synchronize KB** button. Content Analyzer displays the **Synchronize KB** dialog box that shows the Knowledge Base on the left and the associated topic tree on the right.

   See the following figure:



3. Select **Synchronize**. Content Analyzer updates the Knowledge Base with the new topic tree structure and shows the synchronized version in the left pane. The differences between the topic structure in the Knowledge Base and the topic tree are shown at the bottom of the **Synchronize KB** window.
4. To save the synchronized Knowledge Base, select **Save**.

When you synchronize a trained Knowledge Base:

- Content Analyzer retains the training for any topics that still exist in the tree. You will need to incrementally train any new topics, however. Emails cannot be categorized to the new topics until the new topics are properly trained. (For details, see Training a Knowledge Base on page 183.)
- If you have added a language node to the topic tree, Content Analyzer adds the new language to the list of those supported by the Knowledge Base.
- If you have deleted topics from the topic tree associated with the Knowledge Base, after synchronization Content Analyzer will no longer classify emails as belonging to the deleted topics.

Maintaining your samples and sample sets

Over time, some of your sample sets might become outdated as the samples age. Because you cannot add new samples to an existing sample set, you need to replace the outdated sample sets with newer versions. You can use the old sets as the basis for the new ones if there are samples in the old set that are still relevant. For details, see Creating new sample sets from existing sets on page 193.

Similarly, you might want to remove outdated samples from the database so they do not impact search times. Because you cannot remove a sample from the database if it is associated with a sample set, the first thing you need to do is remove the sample from any associated sample sets. For details, see Removing samples on page 195.

You can also remove the outdated sample sets so they no longer appear in the various sample set drop-down lists. For details, see Removing sample sets on page 195.

Examining sample sets

To examine the members of a sample set:

1. Open the Content Analyzer Administrator and select **Sample Management** in the left pane.
2. Select the **Remove Samples** tab.
3. Select the sample set in the **Search Criteria** section, clear all of the other search criteria, and select **Conduct Search**. Content Analyzer displays all of the samples in the sample set in the **Search Results** list.

Tip:
You can also examine sample sets using the **Train and Validate KB** dialog box, as described in Creating new sample sets from existing sets on page 193.

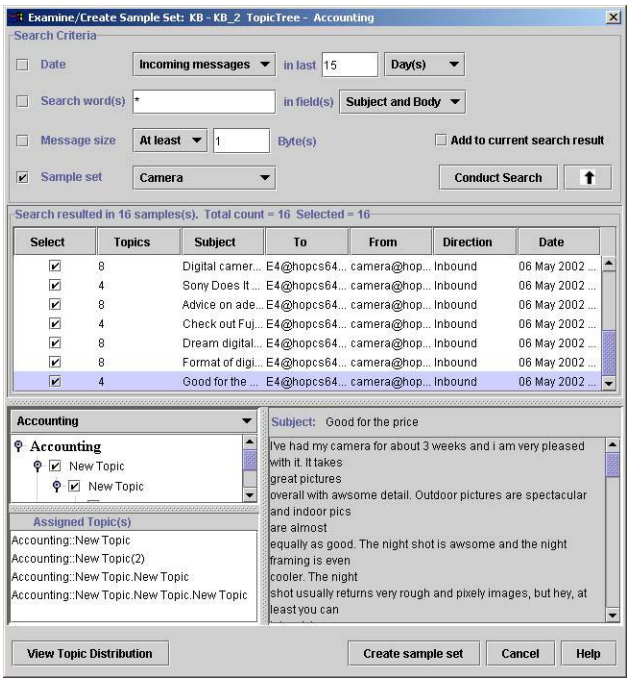
Creating new sample sets from existing sets

You can use a feature in the **Train and Validate KB** dialog box to create a new sample set from existing sample sets. To do so:

1. Select **KB Management** in the left pane, then select a Knowledge Base in the right pane whose topic tree uses the sample set that you want to use as a base for the new set.
2. Select **Train/Validate** in the toolbar. Content Analyzer displays the **Train and Validate KB** dialog box.
3. In the **Training** section, select the sample set you want to use as the basis for the new set from the **Sample Set** drop-down.

4. Select **Examine/Create Set**. Content Analyzer displays the **Examine/Create Sample Set** dialog box with the samples from the selected set already displayed in the **Search Results** list.

   A sample dialog box is shown below:



5. To add more samples to the new sample set, enter the desired search criteria in the **Search Criteria** field, select **Add to current search results**, and select **Conduct Search**.

6. Select the appropriate check box in the search results window for the samples you want to use in the **Search Results** list.

   Tip:
   You can select the check box for all of the samples, the selected samples, the top or bottom 50% of the samples, or the odd or even numbered samples by right-clicking in the **Search Results** list and selecting the appropriate item from the pop-up menu.

7. To view the number of samples assigned to each topic in the topic tree, select **View Topic Distribution** under the topic tree information. Content Analyzer displays the topic distribution for the selected samples in the **Search Results** list. If the distribution needs to be adjusted, select more samples as described in the previous step.

8. To group the selected samples into a sample set, select **Create sample set**. Content Analyzer displays the **Create Sample Set** dialog box. Enter the name of the sample set and then select **OK**. Content Analyzer creates a new sample set containing the samples that you have selected.

Removing sample sets

When you delete a sample set, Content Analyzer deletes the sample set association and the sample set itself, but does not delete the actual samples. For details about deleting a sample from the database, see Removing samples on page 195,

To delete a sample set:

1. Open the Content Analyzer Administrator and select **Sample Management** in the left pane.
2. Select the **Remove Samples** tab.
3. Specify the sample set you want to remove by selecting it from the **Sample Set** drop-down list in the **Search Criteria** section.

   Note:
   If you enter other search criteria, Content Analyzer might show a subset of the samples contained in the selected set. This does not mean that Content Analyzer will only delete the selected samples however. If you delete a sample set, Content Analyzer deletes the entire set, regardless of how many samples are displayed in the **Search Results** list.
4. Select **Conduct Search**.
5. Select **Remove** in the toolbar and confirm the deletion. Content Analyzer removes the sample set and its corresponding sample associations.

Removing samples

You cannot delete a sample from the database if that sample is associated with any sample sets. Therefore, you must first remove all existing sample set associations on a particular sample before you can physically delete it from the database. (For information on removing sample set associations, see Removing sample sets on page 195.)

To remove a sample from the database:

1. Open the Content Analyzer Administrator and select **Sample Management** in the left pane.
2. Select the **Remove Samples** tab.
3. Create a list of samples that you can remove by selecting Not in a sample set from the **Sample Sets** drop-down list in the **Search Criteria** section. You can limit the search results by:
   - Date by selecting the **Date** check box. If you search samples by Date, you can limit the list to incoming or outgoing messages that are older than *n* number of days, months, or years.
   - Search words by selecting the **Search words** check box. If you select this option, you can enter the search words in the associated text field, and then specify whether the words can appear in the subject, body, subject AND body, To address, or From address. If you want to specify that there must be some text in the selected fields but you do not care what the text actually is, enter an asterisk (*) in the **Search words** field.

- Message size by selecting the **Message size** check box. If you select this option, you can specify whether the message should be at least or at most the number of bytes specified in the bytes field.

4. When you have finished adding your search criteria, select **Conduct Search**.
5. When you are satisfied with your search list, select the **Up Arrow** to collapse the **Search Messages** section so that you can view the maximum number of search results at a time.
6. By default, all of the samples in the **Search Results** section are selected. If you want to keep any of the listed samples, clear the check boxes at the beginning of the appropriate list entries to retain those samples.
7. Select **Remove** in the toolbar to delete the selected samples.
8. Confirm the removal at the prompt.

Chapter 8: Avaya IC Report Wizard

The Avaya IC Report Wizard is a user interface for viewing and reporting on the IC Repository database.

Important:
Advanced Reports are End of Sale (EoS) and End of Manufacturing Support. For more details, see the EoS notification at https://downloads.avaya.com/css/P8/documents/101006063. Content present in this document pertaining to 'Advanced Reports' is kept for reference purpose for those who have implemented advanced reports prior to EoS and must not be referenced for any deployments post EoS.

You can use the Report Wizard to:

- Display contact data that was placed in the `repository` database by the Report server.
- Specify the mapping rules that define what data the Report server should store in IC Repository.
- Create and run reports using the Ad-Hoc Report Writer on data in the `repository` database. For details on the Report Writer, see the Report Wizard online help.

Note:
All examples in this section describe the out-of-the-box Avaya IC Report Wizard. Your system may look and function differently from the examples presented if the appearance, format, or settings have been customized.

This section contains the following topics:

- Using the Avaya IC Report Wizard on page 198
- Displaying detailed contact information on page 200
- Specifying what data the Report server collects on page 204
- Modifying creation rules and field expressions on page 208

Using the Avaya IC Report Wizard

To start the Avaya IC Report Wizard application:

1. Select **Start** > **Programs** > **Avaya Interaction Center 7.3.x** > **Report Wizard**.
2. At the database login window, enter your system user name in the **Name** field, and your password in the **Password** field.

Note:
Your user name must have database access to use IC Repository.

3. Select **OK**.
4. Select the **Contact Explorer** or **Mapping Administration** focus.

Note:
For details about using the menus and toolbars in an Avaya IC application, see the Report Wizard online help.

This section contains the following topic:

- The Report Wizard interface on page 199

The Report Wizard interface

The Report Wizard has two focuses:

Contact Explorer focus: When contacts are handled in your contact center, information about those contacts is stored in the `repository` database. The **Contact Explorer** focus helps you:

- perform simple queries to answer questions such as “How many contacts did we handle last year?” and “How many contacts did a particular agent handle on a particular day?”
- follow a contact all the way through the Avaya IC system, including what channels were involved, what queues were used, how long each routing event segment took, and what wrap up codes were associated with the contact
- assess whether you need to add more agents based on the amount of time contacts are spending on hold or in an inactive state
- create ad-hoc reports based on the information in the IC Repository database

For details, see Displaying detailed contact information on page 200.

Mapping Administration focus: To store contact information in your database, you must map contact data to database tables and fields in the `repository` database. The **Mapping Administration** focus helps you define the mapping rules that associate each piece of data with the field it belongs in. This focus is generally used by database administrators and system developers. For details, see Specifying what data the Report server collects on page 204.

Displaying detailed contact information

The Report Wizard's **Contact Explorer** focus displays the details of all the contacts in your IC Repository database based on your specific requirements. You can select one or a combination of the following forms to retrieve the required contact information from the database:

- Contact
- Customer
- Queue

For example, if you select a customer in the **Customer** form and then do a **Search** in the **Contact** form, the Report Wizard displays all of the contacts made by the selected customer.

When you click on a contact in the browser, the Report Wizard backfills the contact information into the **Contact** form, where you can see the details about that contact, such as:

- the type of contact (email, chat, or voice), and the details relevant to the associated channel.
- the agent, or agents, who handled the contact.
- the queue or service class that was used to route the contact to the agent.
- the amount of time the contact spent in the queue, being processed by the agent, and being wrapped up by the agent.
- The wrap up codes associated with the contact by the agent.

This section contains the following topics:

- Contact form on page 200
- Customer form on page 202
- Queue form on page 202
- Retrieving basic contact information on page 202

Contact form

In the **Contact** form, you can view the activities of the agents and the events that occurred while the contact was in the system.

On the **Contact** form, the **Routing Event** group is populated by:

- Telephony (voice) containers with voice event information.
- Email Management containers with email event information.
- Chat containers with chat event information.

Note:
A container is a grouping of values in an EDU under a common name. Some standard containers are maintained by the Avaya IC application. If necessary, you can create additional containers for your application, as described in *Electronic Data Unit Server Programmer Guide*.

Contact group

In Avaya IC, the contact record is the central point to which all aspects of the interaction are linked. Therefore, when you select a contact, you can then access all of the media events that are associated with that contact, all of the agents who participated in that contact, and any other contact-specific information in the Avaya IC database.

The **Contact** group is where you specify what interactions you are interested in viewing. It includes such information as a link to the customer, the date the contact was created, whether the contact was inbound or outbound, and any callback information associated with the contact.

Media Interaction group

This group contains the information that is media instance specific, such as the direction and duration of the media instance. For specific media types, it also has such information as ANI and DNIS for voice contacts, the transcript and user name for chat contacts, and the tracking ID and subject for email contacts.

Note:
For an email, the replies and forwards associated with an inbound email are shown as separate outbound media interaction records on the same contact.

Routing Event group

The routing event stores any information involved with a specific party working the contact. The **Routing Event** group displays the information on routing to the party, as well as the actions of the party in the contact.

Note:
Avaya IC creates a new record for each new party added to the contact.

Task Performed group

This group is used to organize the wrap-up information entered by the agent. It is also a place where task level data can be added for business value reporting or other needs.

Customer form

If your installation uses the CallCenterQ database as the repository for your customer information, the **Customer** form displays information about the customer involved in the contact, such as their name, phone number, and email address.

Queue form

The **Queue** form contains information about the queues where contacts are parked until an agent is available to respond to them. This form includes a subset of the data stored for the queue, including the:

- queue name and ID.
- media type of contacts in the queue.
- site the queue is associated with.
- priority level of contacts assigned to the queue.

Note:
For more information about creating and administering queues, see Devices and queues on page 376.

Retrieving basic contact information

The following examples illustrate how you can access different contact information through the **Contact Explorer** focus using both standard and advanced search constraints. For a detailed list of all the advanced search options in the Report Wizard, see the Report Wizard online help.

Retrieving all customer contacts

To retrieve all contacts made by a specific customer:

1. Go to the **Customer** form and select **Search** in the **Customer** group.
2. Select a customer record from the browser.
3. Go to the **Contact** form and select **Search** in the **Contact** group.

The Report Wizard displays all of the contacts for that customer in the **Contact** browser.

Retrieving all contacts handled by a specific agent

To retrieve all contacts handled by a specific agent:

1. Go to the **Contact** form.
2. In the **Routing Event** group, select the agent in the **Agents** in-form browser.
3. In the **Contact** group, select **Search**.

The Report Wizard displays all of the contacts handled by the agent in the **Contact** browser.

Retrieving contacts by answer time

To retrieve all contacts that took longer than 50 seconds to answer:

1. Go to the **Contact** form.
2. In the **Routing Event** group, enter `>50` in the **Answer Time** field.
3. In the **Contact** group, select **Search**.

The Report Wizard displays all of the contacts that have an answer time greater than 50 seconds in the **Contact** browser.

Retrieving all contacts created since a given date

To retrieve all contacts created since January 1, 2006:

1. Go to the **Contact** form.
2. In the **Contact** group, enter `1 Jan 04..today` in the **Create Time** field and select **Search**.

The Report Wizard displays all of the contacts that were created between January 1, 2006 and today.

Tip:
To display all contacts created in a given week, you can enter `today-7d..today`. If you save this search, you can then rerun it at a later date without having to change a hardcoded start date.

Retrieving all contacts with a specific wrap up code

To retrieve all contacts associated with a specific wrap up code:

1. Go to the **Contact** form.
2. In the **Task Performed** group, select the wrap up code in the **Classification Codes** in-form browser.
3. In the **Contact** group, select **Search**.

The Report Wizard displays all of the contacts associated with that wrap up code in the **Contact** browser.

Specifying what data the Report server collects

The Avaya IC Report server uses rules stored in the `creationrules` and `fieldexpressions` tables to extract the data from an EDU and place it into specific IC Repository database fields.

You can then use Avaya Operational Analyst (Avaya OA) to generate detailed reports on this data to determine the important trends and identify problem areas. For details, see the Avaya OA documentation.

This section contains the following topics:

- Core Tables on page 204
- Reference Tables on page 205
- The Mapping specification on page 206
- Customizing the data model on page 207
- Difference between the EDUID stored in Report Server and DUStore on page 208

Core Tables

For each contact created in Avaya IC, the out-of-the-box creation rules add records to the following IC Repository tables:

```
agentsegment                    routingattempt
contact                         routingevent
mediainteraction                sessionsegment
mediasegment                    taskperformed
                                taskperformedcode
```

For a complete list of the out-of-the-box mapping rules, use the **Mapping Administration** focus. For details, see Viewing and creating rules and expressions on page 210.

The core tables are:

Table Name	Description
contact	A contact is an event that occurs each time a customer establishes communication with the call center. This table contains a record for each initial interaction regardless of how many medias were utilized. It is used for grouping the media instances involved, as well as the agents involved with a specific contact. The data contained is the overall duration and direction of the contact as well as any callback information associated with the contact.
routingevent	A routing event is a record that describes the routing of a contact to a specific agent or autoagent for handling. This table contains a record for each agent or autoagent that handles the contact. There is also duration and counter information summarizing an agent's acceptance, wrap-up information, or active and inactive states on a contact. **Note:** Some standard containers are supplied by Avaya, and you can create additional containers to suit your application. For details, see *Electronic Data Unit Server Programmer Guide*.
agentsegment	The `agentsegment` table has a one to one relationship with the `routingevent` because Avaya IC is actually recording the agent's involvement with the contact. The M:N aspects of this table are not used.
taskperformed	Tasks are specific transactions that are completed to meet a customer's requirement. This table contains a record for each selection made in the agent "wrap-up" dialog providing the category, reason, and outcome codes.

Reference Tables

The data model includes several reference tables. The core tables that are populated by the Report server may include key fields that reference these other tables.

Examples of reference tables are shown in the following table:

Table Name	Description
Customer	A customer is a person or organization that is doing business with an enterprise. This table contains specific information about customers who have previously contacted the contact center.
Agent	An agent is an employee who handles contacts at the contact center. This table contains specific information about the agents working the contact center. For more information about agents, see Managing Agents on page 214.
Product	Information about the products available through the enterprise. **Note:** This information is not populated in the out-of-the-box Avaya IC system.

The Mapping specification

When the Report server starts up, it loads the mappings from the `creationrules` and `fieldexpressions` tables. The Report server takes the terminated EDUs from the EDU server and maps the values to a database. The content of these two tables determine what EDU data is stored.

Creation rules table

The `creationrules` table defines which EDU names will trigger creation of a record in the database.

The names used in these rules can be container names or a wildcard. For example, `voice.*.leg_id` matches every `voice` container with a `leg_id` and creates a database record for each one.

The `creationrules` table contains the following fields:

Field Name	Field Description
pkey*	key
tablename	The name of the table to receive the record.
creationrule	The pattern to trigger the record creation.

Field expressions table

The `fieldexpressions` table defines how to populate the database fields in the table by associating the field name with a matching field or expression in the EDU.

When the associated creation rule uses a wildcard, the field expression can specify an EDU name with the null special token `..` syntax, for example, `voice..connect`. This indicates that for each record created by the creation rule, the Report server should fill in the field with the corresponding value from the same container (`voice.1.connect`, `voice.2.connect`, and so on).

Field expressions can also contain arithmetic expressions, such as the difference between two EDU name values, as well as some functions like `count` (which returns a count of the number of EDU names that match the wildcard). For example: `count(voice.1.hold.*)`. For details, see Field expression functions on page 210.

The `fieldexpressions` table contains the following fields:

Field Name	Field Description
pkey*	key
creatrules_key	The foreign key of the creation rule.
fieldname	The name of the field.
fieldvalue	The expression of the field contents.

Customizing the data model

Customizing the IC Repository data model and setting up the mapping process is very important, as the out-of-the-box EDU values the Report server extracts may not provide enough information for your contact center.

Avaya IC lets you customize the data model and the data extraction process so that you can store whatever information you need from the EDUs available in your Avaya IC system.

Note:
The contents of EDUs can vary greatly from site to site and only some of the EDU names are standard across all switches. If you want to add information to the creation rules table, make sure that the names you specify are available on all the switches in use at your installation.

You can extract customer-specific information from an EDU by:

1. Using Database Designer to add the fields to the tables and then reconfiguring the database. For details, see *IC Database Designer Application Reference*.
2. Using the **Mapping Administration** focus in the Avaya IC Report Wizard to add rules in the mapping tables to specify how the EDU names map to the new database fields.

   For details, see Modifying creation rules and field expressions on page 208.
3. Restarting the Report server.
4. Modifying the out-of-the-box reports to analyze the customized data. (For details, see the Avaya OA documentation.)

Difference between the EDUID stored in Report Server and DUStore

The Report server stores EDU IDs that have been terminated by the EDU server. This means that either all of the clients of the EDUID have terminated their interest in the EDUID or the EDU server forces a termination of the EDUID. The EDU server issues a `Report.EventsIn` method for a `VDU.end` to the Report server.

If the **Enable Persistence** property for the EDU server has been selected, then the DUStore server stores EDU IDs that are still active. There are clients that still have interest in the EDUID but that need to be moved from the EDU server's memory. The EDU server issues a `DUStore.Store` to the DUStore server and sometimes a `Report.EventsIn` method for a `VDU.auRevoir` to the Report server.

Note:
When all clients of an EDUID stored in the DUStore have terminated interest in the EDUID, the EDU server first retrieves the EDUID from the DUStore (`DUStore.Retrieve`), then the EDU server sends (`Report.EventsIn` for a `VDU.end`) the EDUID to the Report server for proper storage in the IC Repository database.

For details about EDUs and configuring persistence, see *Electronic Data Unit Server Programmer Guide*.

Modifying creation rules and field expressions

The **Configuration** form in the Report Wizard's **Mapping Administration** focus lets you modify the `creationrules` and `fieldexpressions` tables.

The **Configuration** form contains two groups: **Creation Rules** and **Field Expressions**.

Creation Rules group

The **Creation Rules** group contains information about the creation of records for specified tables on the system. The following table describes the fields in the **Creation Rules** group:

Field Name	Description
Create Record in Table	The name of the table where the record will be created.
For Each VDU Entry Matching	The VDU/EDU name that triggers records to be created for the specified table. These EDU names can be wildcards such as *agent.**.

Field Name	Description
Description	A description of the creation rule.
Rulestatus	Whether the rule is active or inactive.
History	The history associated with this record.

Multiple entries are allowed for one table. For example, Agent Event records might be generated by an VRU as well as by an agent. VRUs typically record information in “ivr” or “vru” containers, not in “agent” containers.

Field Expressions group

The **Field Expressions** group contains information about the fields in the table that are populated as a result of adding a new record. The following table describes the fields in the **Field Expressions** group:

Field Name	Description
Populate Field	The name of the field to be populated with data from the EDU.
With VDU Value	The VDU/EDU name value from the EDU server to put into the field. **Note:** EDU names can contain the null special token `..` syntax (for example, `voice..connect`). This indicates that for each record created by the creation rule, the Report server should fill in the field with the corresponding value from the same container (`voice.1.connect`, `voice.2.connect`, and so on). This lets you specify a series of events that can repeat as many times as necessary, and enables the Report server to match each container in the EDU with the record it refers to. For more details, see Field expressions table on page 206.
Created By Rule	A link to the rule that governs this activity.
Description	A description of the field expression.
Rulestatus	Whether the expression is active or inactive.
History	The history associated with this record.

Viewing and creating rules and expressions

To define how the data is mapped to the database, select the table and creation rule in the Creation Rule group and the EDU name in the Field Expression group.

To select the table and creation rule:

1. Select **Search** in the **Creation Rules** group. The browser displays a list of the available tables with their corresponding creation rules.
2. Select a table in this list. The Report Wizard fills in the appropriate fields on the **Configuration** form.

To select the EDU name to trigger the creation of records for the table:

1. Select **Search** in the **Field Expressions** group. The browser displays a list of the fields and expressions for the selected table.
2. Select the field in this list. The Report Wizard fills in the appropriate fields in the **Field Expressions** group.

To apply the mapping configuration to the database:

1. Select **Change** in both groups.
2. Modify the fields.
3. Select **Update** to incorporate the mapping definition, or **Clear** to discard changes.

To create a new creation rule or field expression, select **New**.

Field expression functions

The following expressions can be used in field expressions:

Expression	Description
count(attr)	The number of times a name occurs in the EDU. This would be used with container names which contain wildcards. Thus count(ts.*) would return 3 if there are names “ts.1”, “ts.2” and “ts.3”.
sum(attr)	The sum of values for an attribute or expression. This would be used with container names which contain wildcards. An example would be to add the hold times for a call which would be the expression sum(ts..recon.*) - sum(ts..hold.*).

Expression	Description
ifexist(attr,literal)	Substitute a literal value if an EDU name has an entry in the EDU. This would be useful for EDU names that have an empty value.
exp1r - expr2	The difference between two expressions. This is mainly needed to obtain time intervals from two EDU names, but can also be used with sum().

Other arithmetic expressions (+, *, /) are also permitted.

More complex calculations can be performed when a report is run, or by an IC Script attached to a pre-update trigger on one of the database tables being populated.

Note that the sum() and count() functions can specify EDU names with wildcards. For example, if Agent 1 talked to a customer for 185 seconds and put them on hold twice, once for 15 seconds and once for 25 seconds, and then Agent 2 spoke to that customer for 60 seconds and put them on hold for 5 seconds, the corresponding EDU would contain the following name/value pairs:

- voice.1.talktime = 185
- voice.1.holdtime.1 = 15
- voice.1.holdtime.2 = 25
- voice.2.talktime = 60
- voice.2.holdtime.1 = 5

In the `Routing Event` table, `count(voice..holdtime.*)` would evaluate to 2 for the first record and 1 for the second.

An EDU name in a field expression that contains `..` must match a name (with wildcards) in one of the creation rules for this table. For example, it would not be legal to specify a field value of `agent..wrapup` if the table creation rule is `voice.*.leg_id`. If you want to associate some values from one container, for example, `agent` with a record for another container, for example, `voice` then you need a separate table and a way to link the table records together. This might involve adding an EDU name to assist in the association. For example, an EDU name `agent..voice` could have the same value as `voice..session`, in which case they act as the join between two records.

In the creation rules, tables that specify names with wildcards must also specify the parent table that is linked to. For example, the `Queue` table has `Routing Event` as parent, so all `Queue` records must be linked to the appropriate `Routing Event` record. Alternatively, you could have a special function in the field specifications, `key(parenttable)`, which would be used to fill the foreign key fields. This is only needed if the parent table's key is a serial type, and thus automatically generated. Otherwise, you can fill the fields from an EDU name.

Complex Expressions

The field expressions that are used with Advanced Reporting Tools were designed to handle basic data extraction from the EDU to the IC Repository database. To create more complex expressions, the following two options are available:

- Compute the expression at report time. Usually this computing is done in Cognos. For details, see the Avaya Operational Analyst documentation.
- Write an IC Script function that is fired just prior to the record being updated to fill in the field(s) with the complex expression. For details on writing IC Scripts, see *IC Scripts Language Reference*.

Chapter 9: Managing Agents

An agent account in Avaya Interaction Center (Avaya IC) often belongs to a support person also known as Customer Service Representative. However, the account can also be for any object that can receive tasks, have contacts routed to it, or administer the system. For example, in addition to being a live individual, an agent account on Avaya IC can be an IVR (Interactive Voice Response) entry point, a queue, or an Auto Response facility. Allowing these other entities to be represented as agents facilitates transfers and conferences over Avaya IC.

Agents must be entered into the Avaya IC database before they can use the Avaya IC system. The agent's information is added and maintained through Avaya IC Manager's Agent Manager. To access the Agent Manager, select the Agent tab in the main Avaya IC Manager window. To view a list of agents assigned to a particular workgroup, select that workgroup in the left pane. For details, see Using the Agent Manager on page 215.

Prerequisites

Domains: When you create agents, you must assign them to a domain. Therefore, you should create your domains before you create your agents, or you will have to assign Default Domain to every agent and then reassign them later. For more information about domains, see Chapter 3: Domains on page 52.

Workgroups and Tenants: You may also want to create workgroups and tenants before you create agents. For details, see Chapter 10: Workgroups and tenants on page 240. Your agent population must be organized into workgroups that mirror the organization of your contact center, and that no single workgroup have more than 500 agents assigned to it.

Business Advocate: If your site uses Business Advocate, you need to set up the Logical Resource Manager (LRM) and link groups before you can assign agents to the Business Advocate system. For details, see *IC Business Advocate Configuration and Administration*.

Agent information

When you create an agent, you can specify the following types of information:

- Contact Information: The agent's phone numbers, email addresses, and postal address.

Note:
You should use the Real Time Subsystem for agent states instead of Avaya IC Manager.

- System Identity: The agent's login ID, task load, and task ceiling.
- Membership: The agent's assignment to domains, workgroups, and sites.
- Media Channel Properties: The media channels (voice, email, web) configured for use by the agent.
- Skills: The specific skills and abilities of the agent.
- Advocate information: If your site uses Business Advocate, the LRM and Link group that the agent belongs to.
- Security Attributes: The agent's password and role assignments.

Note:
An agent *must* be assigned one or more roles.

After you have created agent records, Avaya IC Manager needs to commit those records to the database. For details on committing the changes, see Updating the database on page 239.

This section contains the following topics:

- Using the Agent Manager on page 215
- Creating a new agent on page 216
- Adding a non-agent member to the Unified Agent Directory or Address Book on page 236
- Searching for agent records on page 236
- Sorting agent listings on page 237
- Changing agent information on page 237
- Updating the database on page 239
- Deleting an agent on page 239

Using the Agent Manager

The left pane of the Agent Manager lists the existing tenants and workgroups. To view the workgroups assigned to a tenant or workgroup, expand the top-level entity. If a workgroup contains agents and/or queues, information about these agents and queues are displayed on the right pane of the Agent Manager. Agents can only be assigned to workgroups, the workgroups are assigned to tenants.

By default the Agent Manager retrieves agent accounts from the database only when a workgroup is selected. When Avaya IC Manager first displays the Agent Manager, no workgroup is selected so there are no agents listed. To load the agents when Avaya IC Manager starts up, enable the Auto Load option by selecting **Agent** > **Auto Load**.

Tip:
The **Auto Load** option should not be used when there are a large number of agents in the Avaya IC system or Avaya IC Manager will require a prolonged start up time.

The Agent state column in Agent Manager indicates current agent state.

The following table provides information on agent states:

Agent State	Image
Not logged in	
Logged in	
Disabled	
AutoAgent	
AuxWork	
InitAuxwork	

Creating a new agent

Avaya IC Manager allows to create agent accounts using the **Agent Editor**. To do so:

1. Select the **Agent** tab on the Avaya IC Manager window.
2. Select the workgroup from the left pane to which you want to add the agent.

   Note:
   If you create a single workgroup with all of your agents in it, Avaya Agent users may experience long wait times when opening the Unified Agent Directory and selecting agents from that list. Avaya recommends that a single workgroup should contain no more than 500 agents.
3. Select **Agent** > **New**.

   Avaya IC Manager displays the **Agent Editor**.

   Tip:
   Required fields are marked with an asterisk (*) in the Agent Editor.
4. Enter the agent's information in the **Agent Editor**. For details, see:
   - Entering basic agent information on page 217

- Configuring channels on page 223
- Setting agent security information on page 226
- Assigning agent properties on page 230
- Defining agent skills on page 231
- Setting Business Advocate information on page 233
- Setting miscellaneous agent information on page 234

5. After entering information on the tabs, you can:
   a. Create the agent account and return to the Avaya IC Manager window by selecting **OK**.
   b. Create the agent account and keep the **Agent Editor** open and available by selecting **Apply**.
   c. Return to the Avaya IC Manager window without creating the agent account by selecting **Cancel**.

Note:
If you cannot log in as the agent after you create the agent record, stop and then restart the Telephony server. To have this update happen automatically, select **Servers** > **Auto Update**.

Entering basic agent information

Fields and subtabs on the Agent Editor's General tab allows you to define:

- Basic employee information such as name, title, employee ID, and manager. For more information, see Employee information on page 218.
- Personal and business contact information for the agent such as email addresses, telephone numbers, fax numbers, and mailing addresses. For more information, see Contact information on page 218.
- System information such as the login and task settings assigned to the agent's account. For more information, see System information on page 220.
- Membership information for domains, workgroups, and sites. For more information, see Membership information on page 222.
- Additional free-form comments. For more information, see Additional notes on page 223.

You can also use the Agent History subtab to view past changes to this agent's database record. For more information, see Agent history information on page 223.

Note:
In all cases, required fields are marked with an asterisk (*). You must enter data in these fields.

Employee information

The Employee Information section of the Agent Editor's General tab contains the agent's title, name, employee ID, and manager.

To enter Employee Information:

1. Enter the agent's title and name information in the provided fields.
2. Avaya IC Manager automatically copies the agent's first name into the **Preferred Name** field. You can edit this field if you want to use another name.
3. If the **Agent Editor** includes the **Display Name** or prefix, suffix, and salutation fields, enter the agent's name information in these fields. Generally, these fields are used with localized versions of Avaya IC. (For more information on enabling these fields, see Admin/Agent properties on page 570.)
4. Enter the agent's employee ID assigned by the contact center in the **Employee ID** field.

   Avaya IC Manager does not do any validation on this field.

   Note:
   The employee ID is *not* the same as the agent's login ID, although you could use the same alphanumeric string for both. In the Avaya IC system, the employee ID is recorded for informational purposes only, while all application access is based on the agent's login ID. For details about setting the login ID, see System information on page 220.
5. If the agent being added will manage other agents, select the **Is Manager** check box. Otherwise, clear this check box.
6. To select the agent's manager:
   a. Select **Browse** in the **Manager** field.

      Avaya IC Manager displays the **Manager** dialog that provides a list of the agents who are designated as managers within the Avaya IC system. (In other words, this dialog lists all of the agent records that have the **Is Manager** check box selected.) You cannot select a manager who does not already have an Avaya IC agent record.

   b. Select the name of the person who will manage the agent.
   c. Select **OK** to assign this person as the agent's manager.

   Note:
   A supervisor and a manager are considered to be different roles in Avaya IC. An agent can only have one manager, but an agent can have a supervisor for every workgroup to which they belong.

Contact information

The **General** tab of the **Agent Editor** allows you enter personal and business contact information for the agent such as email addresses, telephone numbers, fax numbers, and mailing addresses. Use the **Email**, **Phone**, and **Address** tabs located under the general employee information to enter this information.

To enter email information:

1. Select the **Email** tab on the **Agent Editor**.
2. Enter the agent's complete email addresses for the following email accounts:
   - **Primary**. Assigned to the agent by the contact center. This address is configured at the contact center's mail server. If you specify that the agent is user addressable on the System tab, then Avaya IC will list this email address for the agent in the Agent Directory.
   - **Internal**. Used for internal email messages only, not intended to be used outside of the contact center.
   - **Personal**. The agent's personal email address used for non-business communication.
   - **Mobile Device.** The agent's email address for their mobile device.
3. Select **OK** to save the agent's email information.

To enter phone information:

1. Select the **Phone** tab on the **Agent Editor**.
2. Enter the complete telephone numbers with extensions for this agent in the following fields. Phone numbers can be punctuated with periods, commas, hyphens, and parentheses.
   - **Primary**. Used to reach the agent during business hours
   - **Secondary**. Used if the agent cannot be reached at the primary number.
   - **Mobile**. The agent's mobile (cellular) telephone number
   - **Pager**. The agent's pager number
   - **Home**. Used to reach the agent at home
   - **Fax**. The number where the agent receives faxes.
3. click **OK** to save the agent's phone information.

To enter address information:

1. Select the **Address** tab on the **Agent Editor**.
2. Select the type of address from the drop-down list. You can select **Home**, **Office**, or **Other**.
3. Select **Address**.
4. Enter the appropriate address information for this agent, such as company name, mailstop, street address, city, state, and zip code.
5. Click **OK** to return to the **Agent Editor**.
6. Click **OK** to save the agent's address information.

System information

The System Information section contains the login and task settings assigned to the agent's account. These settings include login ID, auto agent, and task levels. Task levels are used by the routing engine to restrict the number of concurrent contacts the agent can handle. The login ID must be unique (in other words, two agents cannot share the same login ID).

To monitor multiple devices, the agent or supervisor can simultaneously login to more than one workstation. However, you must not use simultaneous logins with the same login ID. The agent or supervisor uses a separate login ID for each system.

Note:
Simultaneous logins with the same login ID can impact the migration scripts.

You must not use:

- Two agents logging in with the same login ID.
- One agent simultaneously logging in to more than one machine with the same login ID.

To enter system information:

1. In the **Login Id** field, enter the unique login ID of an agent.

   IC supports the following criteria for creating in the login ID name of an agent:

   - Only lowercase ASCII characters
   - An underscore ('_') character
   - A decimal digit (Not as the first character)
   - Starts with the alphabetic character
   - Length of the login ID name must be between 1 to 24 characters.

   An agent uses this login ID to access all the Avaya IC components. For information on setting the password for this login Id, see Setting agent security information on page 226.

   Note:
   After you set the login ID for an agent, you cannot change that login ID. You need to create a new agent record with new login ID.

2. Click **Options** to set the options for the agent account.

   You can select:

   - **Software Agent**

     Select this option to designate the account as being a non-human entity, such as an IVR entry queue, server, or auto email handler.

   - **External Agent**

     Select this option if the agent works for a different company or is otherwise outside the Avaya IC system. Creating an external agent account means that the resource can be referenced, tracked, and reported on like a normal agent.

   - **User Addressable**

     Select this option if the agent should be displayed in the Unified Agent Directory for Avaya Agent and the Address book for Avaya Agent Web Client. If selected, other agents can transfer contacts to this agent.

   - **Out of Office**

     Select this option if the agent is unable to handle contacts for a lengthy period of time. If the agent has any currently-assigned emails, Avaya IC Manager removes those emails from the agent's queue and reassigns them to an available resource. (If you select this option for an agent who is currently logged in, Avaya IC Manager does not cancel any of the agent's active tasks. It just redistributes any pending emails and does not assign anything new to that agent.)

   Note:
   The **Out of Office** options works only if IC is integrated with Business Advocate and not supported in a non-advocate mode.

3. When you are done specifying the account's options, click **OK**.
4. Set the **Task Load** field to less than or equal to the sum of channel task loads.
5. Select the arrow keys in the **Task Load** field to set the maximum number of contacts that the agent can handle concurrently. These contacts can come from any of the media channels used by the agent. To define which media channels the agent will use, see Configuring channels on page 223.
6. Select the arrow keys in the **Task Ceiling** field to define 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. To define this limit for each of the media channels, see Configuring channels on page 223.

   Note:
   The standard blending flows do not use the **Task Load** and **Task Ceiling** options for blending. You would have to customize the blending flows to use these options. If you want to use these options, see *Avaya IC Media Workflow Reference*.

Membership information

The agent is assigned to domains, workgroups, and sites in the Membership Information section. When you make membership assignments, you should keep the following things in mind:

- An agent's domain membership defines how the agent communicates with servers and what failover policy applies to the agent. For more information about domains, see Chapter 3: Domains on page 52.
- An agent's workgroup membership is based on the way your business is organized. Agents should be grouped by business functions and the related tasks that they perform. For details, see Chapter 10: Workgroups and tenants on page 240.
- An agent's workgroup memberships are ordered. The top most workgroup is designated as the primary workgroup, and Avaya IC Manager uses this workgroup when routing chat and email contacts. Workgroup ordering helps define the inheritance order of properties with the property inherited from the primary workgroup and its ancestors taking precedence. For details, see Chapter 15: Properties on page 364.
- An agent's site membership defines their physical location. Sites can be used by Avaya IC to make routing decisions on contacts, so they must match the sites assigned to the Web ACD. For details about working with sites, see Managing sites on page 37.

To enter Membership Information:

1. Select the drop-down list in the **Domain** field and select the domain to which you want to assign the agent. (If your environment only contains one domain, Avaya IC Manager automatically uses that domain.) Agents cannot belong to more than one domain. For more information about domains, see Chapter 3: Domains on page 52.

   Note:
   If the agent will handle chat contacts, the agent domain must failover to the domain that includes the Paging server. For more information about servers, see Chapter 4: Managing servers on page 62.

2. Select **Browse** in the **Workgroup** field.

   Avaya IC Manager displays the **Workgroup Membership** dialog and lists the available workgroups in the **Workgroups** pane.

3. Select the name of the desired workgroup in the **Workgroups** field.
4. Select the **Right Arrow** button to assign the agent to the selected workgroup.
5. Repeat steps 3 and 4 for all of the workgroups to which you want to assign an agent.

   Tip:
   Keep in mind that Avaya IC only uses the top-most workgroup to route chat and email contacts to the agent.

6. Select **OK** on the **Workgroup Membership** dialog to save the workgroup assignments and return to the **Agent Editor**.

7. Select the agent's site from the **Site** drop-down list. Avaya IC Manager uses this information to define the agent's physical location for routing purposes.

Additional notes

The **Notes** tab provides a free form text box where you can create and maintain information about individual agents. This information may be anything that helps you supervise the agent such as the agent's work schedule or skills.

To enter agent information at the **Notes** tab:

1. Select the **General** tab of the **Agent Editor**.
2. Select the **Notes** tab.
3. Enter the information that you need for this agent in the text box. You can edit the text later if necessary.
4. Click **OK** to save the information to the agent's record in the database.

Agent history information

The **History** tab displays past changes made to the agent's database record from the employee table. Avaya IC Manager displays the last time the record was changed in the header of the file.

To display agent information at the **History** tab:

1. Select the **General** tab of the **Agent Editor**.
2. Select the **History** tab.
3. Select **Refresh** to display the most recent history for the agent.

   Avaya IC Manager appends the newest information to the bottom of the display.
4. Click **OK** to close the **Agent Editor**.

Configuring channels

The **Channels** tab of the **Agent Editor** lets you configure media channels for the agent to use. Agents can be authorized to use any combination of these channels. By default, all channels are disabled.

Tip:
If the agent is designated as an External Agent, then you should leave all media channels disabled. (For more information on external agents, see System information on page 220.)

To configure media channels for an agent, select the **Channels** tab on the **Agent Editor**. The properties for each channel are displayed when the channel is selected from the **Channel** drop-down list. You can configure the:

- Chat channel
- Email channel
- Voice (telephony) channel

Chat channel

To enable a Chat channel, select **Chat** from the **Channel** drop-down list and clear the **Disable Chat Channel** check box.

You can set the following options for the Chat channel:

Task Load: Specifies the number of chat contacts that the agent can handle concurrently. You can assign all or part of the agent's overall task load (specified in the System information on page 220 section) to this channel. The task load cannot exceed the value in the **Task Ceiling** field.

Task Ceiling: Specifies the maximum number of chat tasks that can be assigned to an agent. If this number exceeds the value specified in the **Task Load** field, then the first *n* chat tasks (where *n* = the task load) will be run concurrently while the rest will be queued.

To save your changes, click **OK**.

Email channel

To enable an Email channel, select **Email** from the **Channel** drop-down list and clear the **Disable Email Channel** check box.

You can set the following Email channel options:

Show Full Headers: To display the entire message header to the agent, select the **Show Full Headers** check box.

From Address: To specify the email address that will appear in the From line on all the emails this agent sends, enter the address in the **From Address** field. The email address must be compliant with the RFC 2822 standard. For example agent6@company.com Or Agent_Name <agent@company.com>.

Note:
If the **From Address** is not compliant with the RFC 2822 standard, then ICEmail Server will not process outbound emails send by an agent. The system also displays an unable to send the email warning message.

Task Load: Specifies the number of email contacts that the agent can handle concurrently. You can assign all or part of the agent's overall task load (specified in the System information section) to this channel. The task load cannot exceed the value in the **Task Ceiling** field.

Task Ceiling: Specifies the maximum number of email tasks that can be assigned to an agent. If this number exceeds the value specified in the **Task Load** field, then Avaya IC considers the first *n* email tasks (where *n* = the task load) to be active while the rest are considered queued.

To save your changes, click **OK**.

Voice (telephony) channel

To enable a Voice channel, select **Voice** from the **Channel** drop-down list and clear the **Disable Voice Channel** check box.

You can specify the following Voice channel options:

Phone ID: The physical teleset extension or the agent login ID.

In a Avaya Communication Manager environment, for EAS agents, the Phone Id is the agent's login ID. For a direct connection (one without any queue involvement), the Phone ID is the physical teleset extension.

Password: Required only when the **Phone Id** field contains an agent ID that has been assigned a password on the switch.

Phone Type: The type of switch connection this agent uses:

- In a Avaya Communication Manager environment where the **Phone ID** contains a login ID, set this to **EAS**.

  Note:
  For Avaya Communication Manager, the phone type **Direct** is not supported with Avaya Agent Web Client, SDK Client, and Siebel Client.

- For a direct line with no queue connection, set this to **Direct**.

Equipment: If you are using:

- A Avaya Communication Manager switch and this is an EAS agent, set this to the physical teleset extension.

Queue: The voice device that this agent is assigned to upon login. The device must reference an ACD queue that has already been created in the ACD. Avaya IC Manager does not instantiate or configure third party ACD queues.

If the ACD queue has not been created, leave this field blank.

Task Load: Specifies the number of voice contacts that the agent can handle concurrently. (It makes sense to enter a value of **1** (one) in this field as agents can only take one phone call at a time.) You can assign all or part of the agent's overall task load (specified in the System information section) to this channel. The task load cannot exceed the value in the **Task Ceiling** field.

Task Ceiling: Specifies the maximum number of voice tasks that can be assigned to an agent. If this number exceeds the value specified in the **Task Load** field, then Avaya IC considers the first *n* voice tasks (where *n* = the task load) to be active while the rest are considered queued. To save your changes, click **OK**.

Setting media channel configuration properties

To set the configuration properties for media channels:

1. Select **Tools** > **Groups**.
2. Select the **Properties** tab to display a list of the items for which you can set properties.
   a. Select **Admin/Agent/Email** from the **Sections** pane to display the properties that are currently set for the email channel.
   b. Select **Admin/Agent/Chat** from the **Sections** pane to display the properties that are currently set for the email channel.
3. Select **Create New Settings** to display the **Assign Property** dialog.
4. Select the **Property** drop-down list. If you are using both of these channels, repeat the process for both channels.
   a. Select **ChannelEnabled** for **Admin/Agent/Email** to enable notification to the email channel.
   b. Select **ChannelEnabled** for **Admin/Agent/Chat** to enable notification to the chat or web channel.
   c. Select the **Yes** option **Property Value** field for each channel.
   d. Click **OK** to set the property and return to the **Group Manager**.
5. Click **OK** in the **Group Manager** to save the admin configuration settings.

Once the properties have been set for the media channels, you must restart Avaya IC Manager for the changes to take effect.

Note:
These changes apply to any new agents that you create after you restart Avaya IC Manager. Avaya IC Manager does *not* retroactively apply them to already existing agents.

Setting agent security information

The Security tab lets you set or modify the password assigned to the agent's login ID (for details, see System information on page 220). You can also use this tab to assign the roles that define the agent's privileges.

For more information, see:

- Agent passwords on page 227

- Agent roles on page 227
- Permissions associated with agent roles on page 228

Agent passwords

To prevent access to Avaya IC by unauthorized users, agents are assigned passwords that are required when they log into Avaya 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 Contact/AgentDesktop property descriptions on page 631.)

To change an agent's password:

1. Select an agent's name at the **Agent Manager**.
2. Select the **Security** tab.
3. Enter the agent's password in the **Password** field. Passwords are case sensitive and *cannot* have leading or trailing spaces. To preserve the security of passwords, Avaya IC encrypts them in the database and masks them in the display field.
4. Re-enter this password in the **Confirm** field.
5. If you want to force the agent to change the assigned password the first time they log in, select the **Force password change on login** check box.

   Note:
   Out-of-the-box, the **Force password change** option does *not* check to make sure that the agent supplies a different password from the one that they are supplied. In other words, the agent could set their personal password to be the same as the one that you assign to them on this tab.

6. If you want to disable this account, select the **Disable Login** check box.

   Note:
   You cannot disable an agent who has email contacts pending. For details about reassigning email contacts, see Working with WebACD tasks on page 84.

7. Click **OK** to save the agent's security information.

Agent roles

Agent roles define privileges within Avaya IC. For example, a supervisor has the authority to change agent records while an agent cannot do so. Every agent record needs to have at least one role associated with it.

CAUTION:
Multiple users must not have permission to modify database information because database corruption can occur. If multiple users have permission to modify database information, you need to organize their roles carefully so that one administrator does not overwrite the changes made by another administrator and risk corrupting the database. Avaya IC Manager does not lock records when you start making changes, so the coordination is entirely up to the administrators.

To assign roles to an Avaya IC user:

1. Select the **Security** tab of the **Agent Editor**.
2. Select the check box for each role to assign to the user. For details about the permissions associated with each role, see Permissions associated with agent roles, below.
3. Select **OK** to assign the selected role(s) to the agent.

Permissions associated with agent roles

Agent roles are organized hierarchically, with the Administrator role at the top and the Agent role at the bottom. Administrators can create, modify, or delete any record within the Avaya IC system, but agents cannot even log in to Avaya IC Manager.

If you assign the Supervisor or Clerk role to a user, he or she can modify any agent records below themselves on the hierarchy, but they cannot modify any agents above them. (So, for example, a clerk cannot change a supervisor, and neither one can change an Administrator.)

In addition, only administrators, supervisors, and clerks can enable or disable agent accounts, create or modify workgroups, or assign roles to agent records. Only administrators can create or modify tenants and wrap up codes.

The following table lists the possible roles in order from maximum authority to minimum authority:

Role	Description
Administrator	Administrators have all system privileges. They can create, update, delete, and monitor all the entities of the Avaya IC system including agents, workgroups, tenants, servers, and queues. Administrators can also perform agent, queue and workgroup assignments, administer scripts, assign supervisor accounts, assign roles to agents, and assign task load and task ceiling values to an agent's activities. **Note:** Only administrators can create or delete tenants or wrap up codes. (For more information, see Tenants on page 241 or Creating wrap up, AuxWork, and Logout codes on page 308.) The are also the only users with complete access to all of the functions within Content Analyzer. For more information, see Chapter 7: Using Content Analyzer for automated email processing on page 170. Administrators can access the Business Advocate Administration tool and view all of the Business Advocate administrative data.
Supervisor	If a supervisor is a member of a workgroup, that supervisor can modify the records of any agents belonging to that workgroup, but he or she cannot modify the agent records for anyone else. This authority is cumulative. Supervisors can change agent records for all agents, except those with Clerk roles, in all the workgroups to which a supervisor belongs. A supervisor can: • create, edit, and delete agent information • assign task load and task ceiling values to an agent's activities • change agent property settings • assign roles to all agents of Supervisor level and below • monitor the agents activities on the system • generate reports • administer the content and resources of the system. Other supervisor duties include creating, updating, and deleting Web Self-Service documents and mail templates, administrating and approving Web Self-Service documents, maintaining Auto Reply and other messages. If you want to have an agent monitor the web chats for a workgroup, then the monitoring agent *must* be a supervisor. Supervisors can access the Business Advocate Administration tool, but they can only view site specific agents and profile data.
Clerk	Clerks can create, delete, and update agent accounts and workgroups. They can assign agents to workgroups, and import and export agent records to and from the system. In addition, they can assign roles to all agents of Clerk level and below.The main difference between clerks and supervisors is that clerks can edit all workgroups and agents, while supervisors can only edit those workgroups to which they belong.

Role	Description
Operator	Operators are responsible for monitoring the status of the Avaya IC servers and can stop and start system servers to resolve problems. They also monitor alarms and server activity on the system.
Editor	Out-of-the-box, Editors enable content analysis administration.
Postmaster	Postmasters supervise email channel tasks for the agent and are authorized to administer Email Filters, Mail Accounts (POP3/SMTP accounts), and Email queue changes.
Support	Support contacts can assist customers who have issues with the company's products. Support contacts do not have permission to log in to Avaya IC Manager.
Agent	Agents can receive tasks from any valid media channel, view personal statistics for the customer, and create and submit new Web Self-Service documents. Agents do not have permission to log into Avaya IC Manager. **Note:** If you are using Avaya Operational Analyst, you must select the Agent role for all agents that you want included in your Avaya OA reports.

Assigning agent properties

Properties are attributes used to customize the agent's Avaya IC environment. For example, properties can be used to define the colors, button appearance, and behavior of the agent's application.

Agents inherit the properties of the workgroup(s) to which they are assigned based on set inheritance rules. Any properties that are directly assigned to an agent override any inherited properties. For details about properties, see Chapter 15: Properties on page 364. For a list of the default Avaya IC properties, see Appendix E: Property descriptions on page 570.

To assign properties directly to an agent:

1. Double-click the agent's name at the **Agent Manager** to display the **Agent Editor**.
2. Select the **Properties** tab.
3. Select the name of the section to which you want to apply the property in the **Sections** pane.
4. Select **Create New Setting** above the **Value** column to display the **Assign Property** dialog.
   a. Select the type of the property from the **Property Type** drop-down list.
   b. Select the property value from **Property Value** drop-down list.
   c. Click **OK** to close the **Create New Property** dialog.
5. Click **OK** to add the property to the agent's record.

Defining agent skills

A skill is any qualification that differentiates agents, such as the ability to speak a foreign language or the ability to process auto loans. Skills are typically based on the business needs of the contact center and its customers. Using these skills, Avaya IC can be configured to route incoming contacts to the appropriate agents.

Note:
Business Advocate does not use Avaya IC Manager skills to route contacts. For details about setting up skill-based routing in Business Advocate, see *IC Business Advocate Configuration and Administration*.

Skill categories can be nested. For example, you could create a Language skill category with subcategories for English, French, German, Japanese, and Spanish.

Skills are specific to the Avaya IC environment, and do not relate to any switch or database configurations.

For more information, see:

- Skill categories on page 231
- Agent-skill associations on page 232

Skill categories

To define a skill category:

1. Select **Tools** > **Skills** from the main Avaya IC Manager window.
2. If you want to create a top-level skill or skill category, select **Skills**. Otherwise, select the existing skill or category under which you want to create a subskill.
3. Select **New**. Avaya IC Manager displays the **Edit Skills** dialog.
4. Enter the name of the skill category or subcategory (up to 32 characters). You cannot use "**/**" as one of the characters.

   Note:
   When you first add a new skill category, Avaya IC Manager treats it as if it were a regular skill and displays the name proceeded by the skill icon. As soon as you select the new category and add a skill under it, Avaya IC Manager changes the skill icon to the skill category icon and promotes the skill to a skill category.

5. Click **OK** to return to the **Skills Editor**.

If you want to add more skills, repeat the above procedure. If you are done, Click **OK** on the **Skills Editor** to save your changes and return to Avaya IC Manager.

Agent-skill associations

Once you have defined skills categories, use the **Skills** tab of the **Agent Editor** to assign them to an agent. Avaya IC Manager requires that you assign skills on an individual agent basis. If you select multiple agents, the **Skills** tab is not available.

The **Defined Skills** pane on the left side of the **Agent Editor** lists the available skills. Skills that have been assigned to this agent are listed in red and are also listed in the **Assigned Skills** pane on the right. The **Proficiency** field defines the level of expertise that the agent has in the skill, with **1** being the lowest level of proficiency.

These panes can be resized by moving the cursor onto the dividing bar and dragging the bar.

To assign skills to an agent:

1. Expand the skill categories in the **Defined Skills** pane to display the available skills as necessary.
2. Select the desired skill and select **New** to add it to this agent's list of assigned skills.

Note:

All skill assignments are assigned a proficiency rating (default: **1**). The minimum for this value is 0 and it is unlimited on the high side. Typically, contact centers use a range of 1 to 10. Increase or decrease the value to reflect the particular agent's expertise in the skill based on the scheme developed at your contact center.

3. To set the agent's proficiency, double-click the skill in the **Assigned Skills** pane.

   Avaya IC Manager displays the **Skill Proficiency Editor**.

   a. Select the **Up** or **Down** arrow in the **Proficiency** field to set the desired proficiency value.

   b. Click **OK** to save the new value and return to the **Agent Editor**.

4. Click **OK** to save the changes to the agent's list of skills.

To delete an assigned skill:

1. Select the skill in the **Assigned Skills** pane.
2. Select **Delete**.

   Avaya IC Manager removes the skill from the pane and disassociates it from the agent.

Setting Business Advocate information

If your site uses Business Advocate to route contacts to agents, you can use the **Advocate** tab to assign agents to a Logical Resource Manager (LRM) and Link group. To do so:

1. Enable the **Activate Advocate** check box.
2. Use the **LRM Name** drop-down list to select the agent's LRM.
3. Use the **Telephony Link Group** drop-down list to select the agent's Link group.

In Interaction Center, Business Advocate administration supports role based administration in addition to segmentation mode. Role based administration limits access to Advocate Supervisor to those users with Administrator role or Supervisor role. These users can access and modify agents and profiles in their site only. The role of the user accessing the Advocate Supervisor is used to determine the data displayed to the user. The site ID is used to segment the data displayed for the agent and profiles on that site.

- Site supervisors can view only agent and profile data for their site. They cannot access other Advocate Supervisor information like service classes, goals, and system options.
- Administrator roles can access all the Advocate Supervisor information including agents, profiles, services classes, goals, and system options.

For details about Business Advocate, see *IC Business Advocate Configuration and Administration*.

Setting miscellaneous agent information

Out-of-the-box, the **Miscellaneous** tab displays some additional agent information from the `employee` table in the database. For information on how to make custom fields appear on this tab, contact Avaya Technical Support.

To edit information for customized agent records in the database:

1. Select the **Miscellaneous** tab on the **Agent Editor** to display the custom field names and their values. The out-of-the-box fields are:
   - **Date Created**: The date the agent record was created. (Display only.)
   - **Date Modified**: The date the agent's record was last modified. (Display only.)
   - **Change Password Date**: The date on which the agent last changed their password. (Display only.)
   - **Failed Login Count**: The number of times the agent has attempted to log in with the wrong password. (Display only.)
   - **Last Login Date**: The date on which the last failed login attempt was made. (Display only.)
   - **Last Failed Login**: The password supplied on the last failed login attempt. (Display only.)
   - **Communication Preference**: The agent's preferred contact method. You can select Phone, Email, Fax, or Pager.
   - **Electronic Sig**: The fully-qualified name of the agent's electronic signature file.
   - **Location**: The agent's location.
   - **Web Page URL**: The agent's personal web page address.
2. Make your desired changes and click **OK** to save your changes.

Creating accounts for non-human agents

The following table describes the minimum accounts required by your Avaya IC system for non-human Avaya IC users.

Important:
Change the password on all accounts created by the seed data that is installed out-of-the-box.

Account	Component	Description	Login
Admin	Avaya IC Manager login	Administration account that you use to log in to Avaya IC Manager and the Configuration Tool when you configure the system. Additional Admin accounts can be created as needed. **Note:** Avaya IC Manager forces you to change the password for this account when you use Avaya IC Manager.	Login: Admin Password: admin
website	Configuration Tool and Avaya IC servers	The website account is created by the installation and configuration data. The Avaya IC components in the DMZ use this account to access other Avaya IC servers. Use this account to configure the Website Web application and Web Management services.	Login: website Password: website
icmbridge	ICM Bridge	The icmbridge account is created by the installation and configuration data. This account has Operator privileges. Include a Workflow server in the same domain as the ICM account. This is the IC Login account that you use to configure the Attribute server. For more information, see IC Installation and Configuration.	Login: icmbridge Password: icmbridge
dcobridge	DCO Bridge	The Java Application Bridge uses the DCO Bridge account to access Avaya IC servers, such as the Data server. Additional DCO Bridge accounts will need to be created if you will run more than one Java Application Bridge. Each Java Application Bridge in an Avaya IC system requires a unique DCO Bridge account. Domain: User1 Role: Agent	Login: dcobridge1 Password: dcobridge1

Adding a non-agent member to the Unified Agent Directory or Address Book

If you want to add a non-agent member to the UAD or Address Book, you can create a software agent for that number and add that agent to the Dial Directory. Non-agent members allow agents to easily access an internal queue (such as a help desk number) or a commonly-called external number (such as a vendor, partner, or support group).

To create a non-agent member:

1. Select the **Agent** tab and select **Agent** > **New**.
2. Enter a first and last name for the agent. (For example, you can use "Technical" and "Support".)
3. In the System Information section:
   a. Enter a Logon ID for the agent in the **Logon ID** field.
   b. Select **Browse** in the **Options** field under **System Information**.
   c. Select the **Software Agent** check box.
   d. Select the **User Addressable** check box.
   e. Click **OK**.
4. Select the **Channels** tab and:
   a. Select **Voice** from the **Channel** drop-down list.
   b. Clear the **Disable Voice Channel** check box.
   c. Select queue from the **Phone Type** drop-down list.
   d. Enter the Local VDN or 10+ Digit number in the **Equipment** field. (For example, 918002422121.)
   e. Click **OK**.
5. Select **Manager** > **Refresh**.
6. Verify that the new record appears.

Searching for agent records

You can use the Find Agents function to search for agent records based on selected criteria. This function lets you quickly locate a group of agent records that you can then view or modify.

To find and display selected agent records:

1. Select the **Agent** tab in the Avaya IC Manager window.

2. Select **Agent** > **Find Agents**.

   Avaya IC Manager displays the **Find Agent's General** and **Agent** tabs.

3. Enter the desired search criteria in the appropriate fields. For more information about these fields, see Entering basic agent information on page 217.

4. Select **Find**.

   Avaya IC Manager closes the **Find Agent** and displays the agent records that match your search criteria in the **Agent Manager**.

Sorting agent listings

Avaya IC Manager allows you sort the list of agents in descending order or by their login ID.

To automatically sort the list by the **Login ID** column, select **Agent** > **Auto Sort**.

To sort the list in descending order:

1. Select the **Name** field in the Column Header.
2. Hold down the **Shift** key and click the left mouse button.

Changing agent information

You can change agent information on the **Agent Editor**.

To change agent information:

1. Select the **Agent** tab in Avaya IC Manager.
2. Select the agent to be modified from the list on the **Agent Manager**.
3. Select **Agent** > **Edit**.
4. Change the agent's information as desired. For details about the fields in these tabs, see:
   - Entering basic agent information on page 217
   - Configuring channels on page 223
   - Setting agent security information on page 226
   - Assigning agent properties on page 230
   - Defining agent skills on page 231
   - Setting Business Advocate information on page 233
   - Setting miscellaneous agent information on page 234

5. After entering information on the tabs, you can:
   a. Save your changes and return to the Avaya IC Manager window by clicking **OK**.
   b. Save your changes and keep the **Agent Editor** open and available by selecting **Apply**.
   c. Return to the Avaya IC Manager window without saving your changes by clicking **Cancel**.

After you have changed agent records, Avaya IC Manager needs to commit those changes to the database. For details, see Updating the database on page 239.

Note:
If you change any agent information, that agent must log out of Avaya IC and then log back in again before the changes will take effect.

If your agents use Avaya Agent Web Client you must go into the JavaAppBridge and refresh the Address Book. If you do not, agents will see old information in their Address Book. If many agents need changes, make all of the changes first before refreshing the Address Book. This will minimize the load on the WebConnector.

Changing multiple agent records

You can change some of the information in multiple agent accounts at the same time. For a selected set of agents, you can change the manager, workgroup, domain, phone type, skills, Business Advocate information, agent status information, security, and channel settings.

Tip:
Selecting a large number of agents can cause the Avaya IC system servers to slow down and tie up the RDBMS while they handle the request. If you are going to work with a large number of agents, Avaya recommends that you do so during off-peak hours.

To change information for multiple agents at one time:

1. Select the agent records to be changed using **Control+click** to select individual records or **Shift+click** to select a contiguous range of records.

   Tip:
   To limit the list of Agents Avaya IC Manager displays in the **Agent Manager**, use the Find Agent function described in Searching for agent records on page 236.

2. Press the **Ctrl** key and select **Agent** > **Edit**.

   Avaya IC Manager displays the **Multi Agent Edit** dialog, with any fields that cannot be edited grayed out. Fields that do not contain the same value across all selected agents are blank.

3. Enter the information to be changed in the available fields.
4. Click **OK** to save your changes, or **Cancel** to discard your changes.

Note:
When you select **Save**, Avaya IC Manager only changes the fields that you have edited. Information in all other fields remains unchanged for each agent.

Updating the database

When changes are made to agent information, those changes must be saved to the database. Changes to agents accounts are maintained in the database in one of two ways:

- If the **Auto Commit** option is selected on the **Agent** menu, Avaya IC Manager automatically writes changes to the database.
- If the **Auto Commit** option is not used, select **Agent** > **Commit**. Avaya IC Manager then saves all changes to the database.

Deleting an agent

To delete an agent account from Avaya IC Manager:

1. Make sure that the agent you want to delete does not have any pending email tasks assigned to them in Avaya IC. You must reassign any pending email contacts before you can delete the agent. For more information, see Working with WebACD tasks on page 84.
2. Select the **Agent** tab on the Avaya IC Manager window.
3. Select the agent to be deleted.
4. Select **Agent** > **Delete**.
5. Click **OK** at the prompt.

Tip:
To delete multiple agents, either use **Shift+click** for non-contiguous list of agents or **Control+click** for a contiguous list of agents, and then click **Delete**.

When you delete an account, Avaya IC Manager no longer displays that account in any agent listing. It does not, however, delete the actual account from the database because that would cause inconsistencies in any historical reports that reference the deleted user. Instead, it marks the login ID as deleted and leaves the account in the database.

Chapter 10: Workgroups and tenants

A workgroup is a set of agents or queues that form a logical grouping. For example, all of the agents who handle tier one support calls could be assigned to one workgroup, while those who handle tier two calls could be assigned to a different one. This helps the system administrator view statistics and reports for each workgroup, as well as for individual agents or queues. It also helps the administrator apply property settings to all of the agents within the group simultaneously instead of needing to apply those settings to each agent individually.

A workgroup can be assigned to only one other workgroup, but multiple workgroups can be assigned to the same workgroup. In the above example, you could create a high-level workgroup called `support`, and assign the `tier_one` and the `tier_two` workgroups to the `support` workgroup. You could not assign `tier_one` or `tier_two` to any other workgroup, but you could add more workgroups to `support`. The `support` workgroup could be assigned to another workgroup called `services`. This way, tier_one is part of services, though not directly assigned to services.

An agent or queue can be assigned to multiple workgroups. For agents, one of those workgroups must be designated as the primary workgroup. Agents can only receive web and email contacts from their primary workgroup.

A tenant is a set of workgroups that fulfill a particular business function. It can be used to define the security and administrative boundaries around data, queues, and content resources. Each workgroup can be assigned to one, and only one, tenant, but agents and queues can be shared across tenants by assigning those resources to multiple workgroups.

Tenants, workgroups, agents, and queues form a hierarchy. You assign tenants to the top-level Avaya IC entity, called **IC**. You cannot rename or delete this top-level entity. You assign workgroups to tenants, and agents and queues to workgroups.

Important:
Business Advocate does not use the queues or workgroups that are created in IC Manager for routing. You do not have to create the Voice, Chat, and Email queues for Business Advocate to route contacts. For Business Advocate, the concept of IC queues and workgroups is replaced by Service Class. For more information, see IC Business Advocate Configuration and Administration.

CAUTION:
Do not delete DefaultTenant. DefaultTenant is required by some functions within Avaya IC Manager.

This section contains the following topics:

- Properties on page 241
- Tenants on page 241
- Workgroups on page 242

- Grouping rules on page 245
- Creating tenants and workgroups on page 245
- Modifying tenants and workgroups on page 250
- Deleting tenants and workgroups on page 251

Properties

Properties are behavior and appearance options that you can define in Avaya IC Manager and then assign to tenants, workgroups, or agents. For example, properties determine the colors that are displayed on the workstation, the shape of the buttons, and the behavior of the agent application. Avaya IC Manager stores the properties in the database so that irrespective of the machine an agent uses, Avaya Agent always appears the same way to each agent.

Properties can be shared by the entities (**IC**, tenants, workgroups, agents) in Avaya IC through inheritance, or they can be set on a per agent basis. For detailed information, see Chapter 15: Properties on page 364.

Tenants

A tenant is a set of workgroups that fulfill a particular business function. It can be used to define the security and administrative boundaries around data, queues, and content resources. Each workgroup can be assigned to only one tenant, but agents and queues can be shared across tenants by assigning those resources to multiple workgroups.

For example, your contact center is outsourcing its resources to provide services to Chicago Bank and Boston Bank. You can set up this part of your organization with two tenants, one for each bank, that contain workgroups for the banking services that you provide. Agents and queues can be assigned to workgroups in both tenants.

Some basic requirements for tenants on Avaya IC:

- Tenants must belong directly to the top-level entity, **IC**, on the Group Manager. They cannot be assigned to other tenants or to workgroups.
- Tenant names must be unique. You can use any name, up to 80 characters long, that is meaningful to your organizational structure. Do not use a dash or underscore or any other special characters (for example, @!#$*&()<>/\[] etc.) when naming tenants in Avaya IC Manager.

Note:
Once a tenant has been created, it can be renamed.

- If you want to delete a tenant, you must first delete all of the entities such as workgroups, agents, and queues assigned to it. You must exercise caution when deleting tenants because of the potential impact it may have on the organizational structure you created within Avaya IC. You cannot delete DefaultTenant because it is required by some functions within Avaya IC Manager.

  Note:
  If you delete a tenant, the actual record is marked as deleted but not actually removed from the database for reporting purposes. Your database administrator might want to purge the deleted records from the database periodically in order to regain that storage space. For more information, see the database administration manual that was provided with your database.

- Tenants are only supported on the email and web channels. You cannot associate a tenant with a voice channel.

Avaya IC Manager provides a default tenant named DefaultTenant. DefaultTenant is automatically assigned to Avaya IC during installation. You can create additional tenants in Avaya IC Manager, but do *not* delete the DefaultTenant as it is required by certain functions in Avaya IC Manager.

Creating a tenant

1. Create the tenant in Avaya IC Manager. For details, see Creating tenants and workgroups on page 245.
2. Customize the tenant's properties. For details, see Tenant websites on page 326.
3. Create customer mail accounts for the tenant in Avaya IC Manager and assign the customer mail accounts to the new tenant. For more information, see Email accounts on page 111.
4. Create chat and email queues for the tenant in Avaya IC Manager. For details, see Creating devices on page 378.
5. Create routing hints for the tenant in Avaya IC Manager. For details, see Tables on page 388.
6. Assign queues, routing hints, and mail accounts to the Root of the tenant FAQ database (for the Web Self-Service feature). For details, see Setting up the Web Self-Service feature on page 320.

Workgroups

Workgroups contain sets of agents and queues that have related responsibilities or properties. While tenants can contain more than one workgroup, workgroups cannot belong to multiple tenants. To assign an agent to work in more than one tenant, you must create a separate workgroup in each tenant and assign the agent to both of those workgroups.

Some basic requirements for workgroups on Avaya IC:

- Workgroups can contain agents, queues, and other workgroups.

- Workgroup names must be unique across all of the workgroups in the **IC** structure, even if workgroups are assigned to different tenants.
- Workgroups can be assigned directly to the top-level entity, **IC**, instead of to a specific tenant. Avaya recommends direct assignment to **IC** only if your site is not using the tenant feature, or for those workgroups that do not have specific tenant requirements.

You can view and change the hierarchical relationship between **IC**, tenants, workgroups, agents, and queues in the Group Manager by selecting **Tools** > **Groups** from the main Avaya IC Manager window. For details, see Creating tenants and workgroups on page 245. For an example of how you might organize your Avaya IC environment, see Sample organization on page 244.

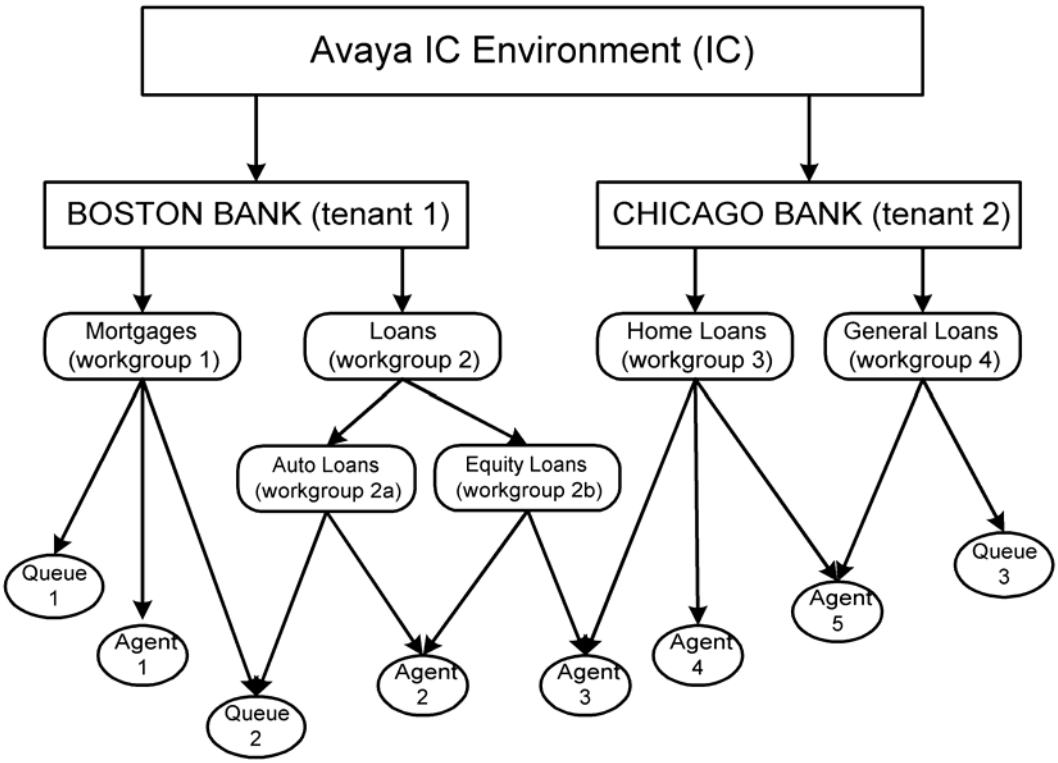
After the workgroups have been assigned to tenants, you can assign agents and queues to these workgroups based on their skills. Agents with skills in multiple areas of service can be assigned to multiple workgroups to fully utilize their time. For more information about assigning agents to workgroups, see Creating a new agent on page 216. For more information about defining agent skills, see Defining agent skills on page 231.

CAUTION:
Do not modify the Default group name. The Default group name is required by some functions within Avaya IC Manager. This may result WACD to end on starting up.

Note:
If you create a single workgroup with all of your agents in it, Avaya Agent users may experience long wait times when opening the Unified Agent Directory and selecting agents from that list. A single workgroup must not contain more than 500 agents.

Sample organization

In the following example, you are outsourcing your resources to provide services to Boston Bank and Chicago Bank. This diagram illustrates the organization of the tenants and workgroups based on the expected number of contacts to be handled from these two different sized banks.



In this example there are two tenants assigned to the **IC** entity for Boston Bank and Chicago Bank:

- Each of these tenants contains workgroups for Mortgages (Home Loans) and Loans (General Loans) services. These workgroups have unique names within each tenant but they perform the same functions.
- Workgroup 2 (Loans) has sub-workgroups for Auto Loans and Equity Loans services.
- Agent 1 is skilled in Mortgages and is handling contacts for Boston Bank. This agent is using Queue 1 and Queue 2 to handle contacts.
- Agent 2 is handling contacts in Auto Loans and Equity Loans across multiple workgroups for Boston Bank and is using Queue 2 for Auto Loans contacts. One of the workgroups will be considered the primary group. In non-Advocate deployments, email and chat delivery will be based on membership to this workgroup.
- Queue 2 is used by agents servicing Mortgages and Auto Loans in different workgroups.

- Agent 3 is handling Equity Loans for Boston Bank and Home Loans for Chicago Bank. Through these workgroup assignments, this agent is working in both tenants.
- Agent 4 is handling Home Loans for Chicago Bank.
- Agent 5 is handling both Home Loans and General Loans for Chicago Bank and is using Queue 3 to help handle the high volume of General Loans related contacts.

Grouping rules

When creating the organizational structure of tenants, workgroups, agents, and queues, remember to follow these rules:

- Workgroups must have unique names even if they are assigned to different tenants within **IC**.
- Workgroups can only be assigned to one other entity in the structure. That entity can be another workgroup, a tenant, or **IC**.
- You cannot define a cyclical relationships for workgroups. In other words, if Workgroup B is a assigned to Workgroup A (making A the parent workgroup for B), you cannot also assign Workgroup A to Workgroup B, which would make B the parent for A.
- Agents and queues must be assigned to workgroups. They cannot be assigned directly to a tenant or to **IC**. Agents and queues can be assigned to multiple workgroups across different tenants.
- Property inheritance is performed top-down. This means that if a property is assigned directly to a workgroup, the direct setting will override any settings that the workgroup might have inherited from **IC** or the tenant to which it is assigned. Similarly, the properties assigned directly to an agent override any settings the agent might have inherited from **IC**, the tenants, or the workgroups to which the agent is assigned. For details, see Property inheritance on page 365.
- The order in which properties are inherited is determined by an agent's workgroup memberships. The primary workgroup is at the highest level of inheritance, followed by the secondary workgroup, and so on. For details about assigning agents to workgroups, see Membership information on page 222.

Creating tenants and workgroups

When Avaya IC and Avaya IC Manager are installed, the installation creates a tenant named DefaultTenant under Avaya IC. The installation also creates a workgroup named Default group under IC. (For more information, see IC Installation and Configuration.) You can create additional tenants and workgroups for your business.

When you create a new tenant, Avaya IC Manager uses the settings for the DefaultTenant as the foundation for the new tenant. When you create a new workgroup, Avaya IC Manager uses the settings for the Default group as the foundation for the new workgroup.

To create a tenant or workgroup:

1. Select **Tools** > **Groups** in the Avaya IC Manager window. Avaya IC Manager displays the **Group Manager** window.
2. In the left pane of the window, Avaya IC Manager displays the organization of the Avaya IC environment with **IC** at the top level.
3. Select **IC** to assign a new tenant or workgroup to the top level of the Avaya IC environment, or select the name of a tenant or workgroup in the organization to designate it as the parent of the workgroup that is being created. Two tabs are displayed in the right pane:
   - **Membership**. Lists all the tenants, workgroups, agents, or queues that are members of the selected parent.
   - **Properties**. Helps you assign properties to the selected entity.

Creating tenants

1. Select **IC** in the left pane of the **Group Manager**.
2. Select the **Membership** tab.
3. Select **Create New Tenant**.
4. Enter the name and description of the tenant in the appropriate fields.

   Do not use a dash or an underscore in the tenant's name. (For example, do not use `default_tenant` or `default-tenant`.) You cannot use any special characters, for example, @!#$*&()<>/\[], when naming tenants in Avaya IC Manager.

   In addition, make sure that you do not reuse a tenant name even if you change the case of the letters within that name. For example, do not use both `DefaultTenant` and `defaultTenant`. Both of these issues can cause problems with the WebACD server.
5. Select **OK** to create the new tenant.

Creating workgroups

1. In the left pane of **Group Manager**, select the tenant or workgroup to which you want to assign the new workgroup.
2. Select the **Membership** tab.
3. Select **Create New Workgroup**.

4. Click the **Properties** tab.
5. In the **Workgroup Name** field, type the workgroup name.

   Do not use a dash or an underscore in the workgroup's name. (For example, do not use **default_workgroup** or **default-workgroup**.) In addition, make sure that you do not reuse a workgroup name even if you change the case of the letters within that name. (For example, do not use both **DefaultWorkgroup** and **defaultWorkgroup**.) Both of these issues can cause problems with the WebACD server.
6. In the **Description** field, type the description for the workgroup.
7. Click the **Supervisor** tab.

   If there are any agents already defined as supervisors in the Avaya IC system, the **Assign from this list** field displays the supervisors.

   For information about assigning agents a supervisory role, see Agent roles on page 227.

   From Avaya IC 7.3.5 onwards, multiple supervisors can be assigned to a single workgroup and a single supervisor can be assigned to multiple workgroups.
8. To assign a supervisor to a workgroup, select the supervisor from the **Assign from this list** field and click the **Assign Supervisor to Workgroup** (**<<**) arrow. The selected supervisor moves under the **Assigned Supervisors** field.

   The maximum number of supervisors assigned to a workgroup is 4.

   To remove a supervisor to a workgroup, select the supervisor from the **Assigned Supervisors** field and click the **De-assign Supervisor** (**>>**) arrow. The selected supervisors move under the **Assign from this list** field.

   Note:
   From Avaya IC 7.3.5 onwards, multiple supervisors assigned to a workgroup can monitor chat for the agents in that workgroup.
9. From the **Default Supervisor** drop-down list, select one of the assigned supervisors as the default supervisor for the workgroup.

   Note:
   From IC Release 7.3.5, all supervisors from the assigned supervisors list can monitor an agent logged in to Avaya Agent Rich Client (AARC). Avaya Agent Web Client (AAWC) and SDK client use the default supervisor you select from the assigned supervisors list for agent monitoring purposes.
10. Select **OK** to create the new workgroup.

Assigning tenant and workgroup properties

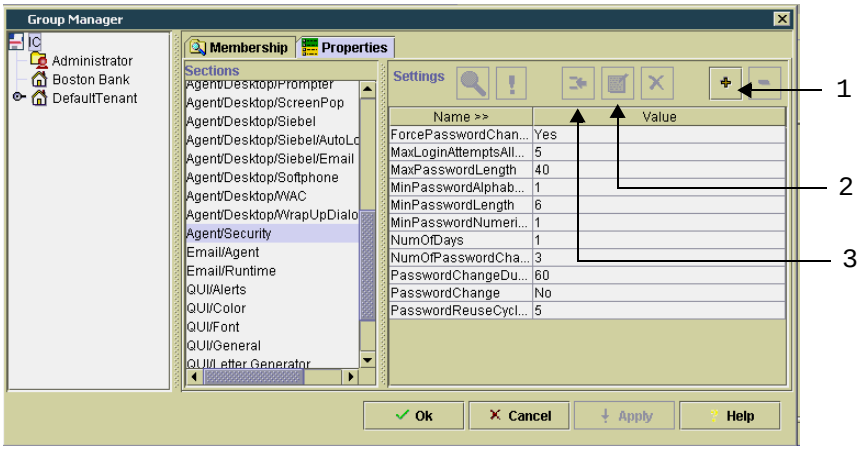
After creating tenants and workgroups, you can assign properties to them. Setting properties for tenants and workgroups enables you to assign and maintain their capabilities in a central location making them easier to manage.

The properties provided with Avaya IC Manager are listed in the Sections pane when **IC** is selected in the left pane. For information about creating and managing properties, see Chapter 15: Properties on page 364. For descriptions of the Avaya IC Manager default properties, see Property descriptions on page 570.

To assign properties to tenants and workgroups:

1. Select the button next to the entity name in the left pane to display its members.
2. Select the member of the entity in the left pane to which you want to assign properties.
3. Select the **Membership** tab to display the members of the selected entity.
4. Select the **Properties** tab.

   Avaya IC Manager displays the Group Manager.



1. Show Inherited Sections/Settings
2. Edit
3. Create New Setting

5. Select the section from the **Sections** pane and select **Create New Setting**.

   Avaya IC Manager displays the **Assign Property** dialog.
6. Select the **Property** drop-down list to display the properties that are grouped into this section, but have not been assigned to the selected entity.
7. Select the property to assign to the tenant or workgroup.
8. Select the **Property Value** drop-down list to display a list of values for the selected property. If there are no values listed, enter a value.

9. Select the value that you want to assign to the property.
10. Select the **Descendants May Override** option for non-cumulative properties. (If a new value for this property is encountered further down the inheritance path, the new value will replace this value. For details, see Non-cumulative property inheritance on page 366.)

    Clear the **Descendants May Override** option for cumulative properties. (If a new value for this property is encountered further down the inheritance path, the new value will be retained along with this value. For details, see Cumulative property inheritance on page 365.)
11. Select **OK** to add the property to the tenant or workstation.

Displaying inheritance information

You must carefully plan the assignment of properties to the Avaya IC entities because many conflicts can arise. You need to understand the tasks that need to be performed and the personnel that are available to do them.

After you have assigned properties to the tenants and workgroups at the contact center, you may want to evaluate the results. Avaya IC Manager lets you display a list of inherited properties for each property section. Furthermore, you can display details for any of the properties on this list. These options can be helpful as you try to make property assignment decisions and resolve property conflicts.

To display information about properties assigned to a tenant or workgroup

1. Select the tenant or workgroup in the left pane of the **Group Manager**.
2. Select the **Properties** tab.
3. Select **Show Inherited Sections/Settings** to display a list of the properties assigned to the selected section in the **Settings** pane.
4. Select the appropriate section from the list of sections for the selected tenant or workgroup from the **Sections** area of the screen.
5. In the **Settings** area of the screen, Avaya IC Manager displays all of the property settings that are inherited by the selected tenant or workgroup from the top down of the workgroup path.
6. Each of the property settings assigned to the section contains a symbol that identifies status information about the property. These symbols are:
   - **Plus sign (+)**. A cumulative property that is accumulated with other properties as it is inherited down the workgroup path.
   - **Question Mark (?)**. A conflict exists between the value of the property for different entities. Select Details to display more information.
   - **Exclamation Point (!)**. A non-cumulative property. There is another value for this property down the inheritance path that replaces this value. Select **Details** to display more information.
   - **Down Arrow.** An inherited property value. This value was assigned at a higher level and not at the local level of this entity.

- **Hyphen (-)**. A local property not inherited from an ancestor entity.

7. The property list also contains the property name, the name of the entity from which the value is inherited, the property value assigned to it, and its override setting (yes or no). You may see multiple values for any given property.
8. To resolve issues due to property conflicts and overrides, select a property with conflicts (**?**) or overrides (**!**) symbol and select **Property Setting Details**. Avaya IC Manager displays the **Details** window.

   The **Details** window contains **Conflicts With** and **Overridden By** sections that provide pertinent information that enables you to resolve property conflicts. Review the information on the **Details** window to understand the status of the property in question.
9. Select **OK** to close the **Details** window.
10. Select **Hide Inherited Sections/Settings** to display the local sections and property values.
11. Select **Undefined Properties for Section** to display a list of the properties currently missing from a value. These properties were added to the value when the value was created with a required attribute selected. You can correct these omissions using this list.

Modifying tenants and workgroups

Avaya IC Manager helps you modify the name and description of workgroups. Tenants cannot be renamed.

CAUTION:
Before you change the name of a workgroup used by the WebACD server, make sure no tasks are currently assigned to that workgroup. If there are, those tasks will be reassigned to the Default workgroup when the WebACD server restarts.

To modify a tenant or workgroup:

1. Select **Tools** > **Groups**.

   Avaya IC Manager displays the **Group Manager** window.
2. Select **IC** in the left pane to display a list of the tenants and workgroups on Avaya IC.
3. Select the tenant or workgroup to be edited from the **Membership** tab.
4. Select **Edit**.

   Avaya IC Manager displays the **Edit Tenant** or **Edit Workgroup** dialog.
5. Edit the information for the tenant or workgroup at this dialog. Select **OK**.
6. Select **OK** on the **Group Manager** to save the changes to the record.
7. If the workgroup is used by the WebACD server, stop and then restart that server.

Deleting tenants and workgroups

Avaya IC Manager lets you delete existing tenants and workgroups. Tenants cannot be deleted if they contain member workgroups. You must delete the workgroups before you can delete the tenant.

CAUTION:
Deleting tenants and workgroups has an impact on the resources that are assigned to tenants and workgroups. For example, the active queues in a workgroup may contain contacts, which should be handled or deleted before deleting the workgroup. Workgroups must be deleted prior to deleting their parent tenants.

To delete a tenant or workgroup:

1. Select **Tools** > **Groups**.

   Avaya IC Manager displays the **Group Manager**.
2. Select **IC** in the left pane to display a list of the tenants and workgroups on the system.
3. Select the name of a tenant or workgroup in the organization that is the parent of the tenant or workgroup that you want to delete.
4. Select the tenant or workgroup to be deleted from the **Membership** tab.
5. Select **Delete** to remove the tenant or workgroup from the list. This does not delete the workgroup or tenant from Avaya IC, it removes it as a member of the selected entity.
6. Select **OK** at the **Group Manager** to complete the removal of the tenant or workgroup from the entity.

Chapter 11: Avaya IC Customer HTML Chat Client

The Avaya IC Customer HTML Chat Client provides chat features without requiring to have or to install a JVM for contact center customers before they can chat with an agent.

This section provides information about the Customer HTML client and how to install, configure, and customize it.

This section includes the following topics:

- About the Customer HTML Chat Client on page 252.
- Required software for the Customer HTML Chat Client on page 255.
- Customizing tenant website properties on page 256.
- Emoticons on page 277
- Chat typing status on page 278
- Configuring blind chat transfer on page 281
- Example: Changing the images for a button on page 282.
- Localization properties on page 283.
- Troubleshooting the Website Multi-Tenant Administration pages on page 285,
- Troubleshooting the Customer HTML Chat Client on page 286

About the Customer HTML Chat Client

The Customer HTML Chat Client is available with Avaya Web Management (Web Management). The Customer HTML Chat Client provides functionality in an HTML format that does not require contact center customers to install the Sun JVM on their machines before they can chat with an agent.

This section includes the following topics that describe the Customer HTML Chat Client:

- Chat features supported by the Customer HTML Chat Client on page 253.
- Limitations of the Customer HTML Chat Client on page 255.

Chat features supported by the Customer HTML Chat Client

The Customer HTML Chat Client supports the chat features described in the following table.

Chat feature	Description
Text chat	Agents and contact center customers can participate in an interactive, real-time text chat session.
Real-time chat transcript	A real-time transcript of the chat is visible in the Customer HTML Chat Client throughout the chat session. At the end of the chat session, the Customer HTML Chat Client remains open to allow the customer to review the chat transcript, if desired.
Emailed chat transcript	A customer can obtain an email transcript of a chat. The customer must check and complete the **Send transcript to** fields when requesting a chat session to obtain a transcript.
Page Push	An interactive "sharing" of Web pages where: • The customer can send a URL that opens a Web page in a browser on the agent desktop. • The agent can send a URL that opens a Web page in a browser on the customer's desktop.
Join Us	An agent can invite one or more people to join the chat session on behalf of the customer.
Survey or follow-up Web page	An optional Web page that can load in the customer browser after the chat session where the customer can complete a survey or provide follow-up information.
Supervisor monitoring	A contact center supervisor can monitor the chat session between a customer and an agent from the Web Agent application.
Emoticons	You can enter the configured sequence of characters in the message area of chat application and the related image is displayed in the transcript area of all the parties involved in the conversation. For more information, see Emoticons on page 277.

Chat feature	Description
Chat typing status	The Chat client displays the chat typing status of an agent to a customer and chat typing status of a customer to an agent. For more information about configuring the chat typing status, see Chat typing status on page 278.
Blind transfer	The Chat client displays a transfer message to the customer when an agent performs a blind transfer. For more information about configuring blind transfer, see .Configuring blind chat transfer on page 281.

Customization features of the Customer HTML Chat Client

The Customer HTML Chat Client includes the following features that allow you to customize its appearance and behavior. For more information, see Customizing tenant website properties on page 256.

Chat feature	Description
Display options	Select one of the following options to display the Customer HTML Chat Client: ● Integrated (docked) window that displays as a frame in the Avaya IC Website. ● Separate pop-up window that opens in a new browser window.
Security options	If desired, use HTTPS protocol for the Customer HTML Chat Client and keep the data in the chat session secure. **Note:** A contact center must purchase a security certificate from a certificate authority such as Verisign or Thawte to use HTTPS protocol.
Customizable appearance	Customize the appearance of the Customer HTML Chat Client, including the company logo, the colors, and the fonts.
Customization by Website tenant	Create a different customized version of the Customer HTML Chat Client for each tenant of the Avaya IC Website.
Customizable transcript format	Customize the format of the transcript as it displays in the Customer HTML Chat Client.
Disconnection limit	Set the maximum time in seconds for a customer who loses a chat session to return to the chat session.

Chat feature	Description
Configurable error messages	Customize the text of any alert that is given during a chat session.
Debug window	Open a debug window in the Customer HTML Chat Client in your development environment to log all trace messages.

Limitations of the Customer HTML Chat Client

The Customer HTML Chat Client does not support the features described in the following table.

Chat feature	Description
Request for chat transcript after chat session closes	The customer must check and complete the **Send transcript to** fields when requesting a chat session to obtain a transcript. After the chat session is closed, the agent cannot obtain a copy of the transcript to send to the customer.

Required software for the Customer HTML Chat Client

This section includes the following topics that describe the Avaya IC servers and software required by the Customer HTML Chat Client:

- Required Avaya IC servers and prerequisites on page 255.
- Supported Web browsers for Website customers on page 256.

Required Avaya IC servers and prerequisites

The Customer HTML Chat Client requires the same Avaya IC servers and prerequisite software as other Web Management features. For more information, see *IC Installation Planning and Prerequisites*.

Supported Web browsers for Website customers

Customers of your Website must have a supported Web browser to use the features of Web Management. This section includes the following topics:

- Supported Web browsers on page 256.
- Customizing tenant website properties on page 256.

Supported Web browsers

For details about the supported versions of the Web browsers and subsequent updates or services packs of the software, see *IC Installation Planning and Prerequisites*.

Customizing tenant website properties

You can use the Customer HTML Chat Client in your contact center without customization. This section provides information on how to customize the tenant website properties for the Customer HTML Chat Client. For example, you can customize the appearance of the Customer HTML Chat Client to use your company logo or color scheme.

Tip:
For more information about tenant website properties and how to customize them, see Chapter 14: Tenant websites on page 326.

This section includes the following topics:

- Modifying the tenant website properties on page 257
- Configuring the chat client deployment on page 259
- Configuring Page Push from customers on page 260
- Modifying the Collaborative Form-filling properties for customers on page 260
- Changing the HTML Chat Client properties on page 262
- Customizing the logo on page 263
- Changing the window position and size on page 264
- Changing the frame sizes on page 265
- Customizing the background colors on page 266
- Customizing the text entry fields on page 266
- Customizing the welcome message on page 266

- Customizing the chat transcript on page 267
- Customizing the timestamp on chat transcripts on page 273
- Customizing the tooltips on page 274
- Adding a help file on page 275
- Enabling the debug window on page 276
- Disabling the Enter event on page 276

Modifying the tenant website properties

The IC Website Administration Tool lets you modify all tenant website properties. This section provides information about how to access and modify the tenant website properties for the Customer HTML Chat Client.

To modify the tenant website properties:

1. In IC Manager, select **Services** > **MultiTenancy Administration**.
2. In the left pane of the **Interaction Center Website Multi-Tenant Administration** page, click **Tenant Properties**.
3. In the right pane:
   a. From **Select a Tenant** drop-down list, select the tenant for which you want to configure the chat client deployment.
   b. Select **Customize Tenant**.
4. In the right pane:
   a. From **Select language** drop-down list, select the language supported on this tenant.
   b. Under **All properties**, click **chat**.
5. Modify the desired properties, as described in the following sections.
6. After you change the desired tenant website properties, select **Update Data**.

Using Macros in chat properties

You can use the following macros in the chat properties:

- $agentid$
- $agentname$
- $callername$
- $callerid$

You can use any combination of macro $agentname$/$agentid$ for the following properties:

- chat.phrases.AgentEnter= Agent $agentname$ enters the call ($agentid$ can also be used)
- chat.phrases.AgentLeft = Agent $agentname$ left the call ($agentid$ can also be used)
- chat.phrases.AgentSetVisible = Supervisor is available on the call. (Here $agentid$ or $agentname$ can be used)
- chat.phrases.AgentSetInvisible= Supervisor is not available on the call (Here $agentid$ or $agentname$ can be used)

You can use any combination of macro $callername$/$callerid$ in the following properties:

- chat.phrases.CallerDropped = Caller $callername$ left the call. ($callerid$ can also be used)
- chat.phrases.callJoined = Caller $callername$ joined the call. ($callerid$ can also be used)

Note:

1. If the administrator uses any macro that is not mentioned above (some custom macro) then the icm server will not replace the macro value.
2. If the administrator uses any macro in a chat property which not mentioned above then the icm server will not replace the macro value.
3. If the administrator defines any agent macro (macro mentioned above) in the caller chat property or caller macro in the agent property mentioned above then the icm server will not replace the macro value.

Modifying the CSPortal chat window idle timeout

In IC 7.3.3 and later, the website administrator can configure the maximum idle time for which the customer remains in an active chat. A message is shown to the customer with the countdown timer which turns the color of the status bar as the time approaches 0 after which the chat is automatically disconnected.

To configure the CSPortal chat window idle timeout:

1. Login to the IC Admin Website as an administrator.
2. Goto the following location:

   http://<machine-hosting-admin-site>:port-number/website/admin/tenancy/addmd.jsp

3. In the Add Metadata page, provide the following details:

Metadata name	Default values	Description	Tenant Property
chat.htmlclient.customer.inactivitytimer.enabled	false	This flag determines whether chat inactivity timer is enabled or is disabled. Valid values are true/false	Yes
chat.htmlclient.customer.inactivity.total time	10	Total time (in minutes) that an active ongoing chat can continue without getting disconnected owing to customer inactivity. Minimum value can be 1 minute.	Yes
chat.htmlclient.customer.inactivity.countdowntime	60	The value (in secs) determines the time duration for which a inactivity warning messsage would be displayed to the customer.Default is 60 secs.	Yes

4. After adding the above Metadata, administrator can configure the idle timeout feature for individual tenants.
5. Restart the Tomcat server that is hosting the Admin Website.
6. Restart the CSPortal server hosted on Tomcat server.

Configuring the chat client deployment

By default, the Customer HTML Chat Client patch configures the Website to deploy only the Customer HTML Chat Client. You can change this deployment, if desired. If your Avaya IC system includes multiple tenants, you can configure a different chat client deployment for each tenant.

To configure the chat client deployment, modify the tenant website properties in the following table:

Customer HTML Chat Client	
chat.htmlclient.enabled	true
chat.downloadjvm	false

Configuring Page Push from customers

By default, Website customers can send URLs to agents in a chat session, also known as Page Push. You can turn off Page Push, and configure which protocols can be used to send URLs.

To configure Page Push, modify the tenant website properties in the following table:

Property	Description	Possible values	Default
chat.htmlclient. sendurl.enabled	Enables and disables Page Push from the customer to agent.	True False	True Page Push is enabled.
chat.htmlclient. sendurl. allowedprotocols	Specifies the valid protocols for URLs in Page Push. Multiple protocols must be separated with a comma. If you enable Page Push, Avaya IC automatically pushes a text message that begins with the protocols specified in the list.	Standard HTML protocols such as: http:// or www.	http://, https://,www.

Modifying the Collaborative Form-filling properties for customers

By default, Collaborative Form-filling is enabled. However you can customize the Collaborative Form-filling properties.

The website customer must have Java plug-in for the Internet Explorer browser to use the Collaborative Form-filling feature. For more details about the definition of supported versions and about subsequent updates or service packs of the Java plug-in for the Internet Explorer browser, see *IC Installation Planning and Prerequisites*.

To customize Collaborative Form-filling, modify the following properties:

Property	Description	Possible values	Default
chat.htmlclient.collaboration.dataPollInterval	The collaborative form data will be exchanged as specified by this poll-interval.	A number greater than zero.	4 seconds. Recommended: Maximum: 8 seconds Minimum: 4 seconds **Note:** A poll interval of less than 4 seconds can overload the Applet.
chat.htmlclient.collaboration.debug	To enable or disable collaboration debugging.	True False	False
chat.htmlclient.collaboration.enabled	To enable or disable the client-side collaboration.	True False	True

Modifying the Collaborative Form-Filling properties for Workgroups and Agents

Workgroup: Configuring the collaboration for a workgroup enables the collaboration for all the agents in that workgroup.

Individual Agent: Configuring the collaboration for an individual agent enables the collaboration only for that particular agent.

Section	Property	Description	Possible values	Default
Agent\Desktop\Chat	CollaborationEnabled	To enable or disable the agent-side collaboration.	Yes No	Yes

Section	Property	Description	Possible values	Default
Agent\ Desktop\Chat	CollaborationPollInterval	The collaborative form data will be exchanged as specified by this poll-interval.	A number greater than zero.	4 seconds. Recommended: Maximum: 8 seconds Minimum: 4 seconds **Note:** A poll interval of less than 4 seconds can overload the Applet.
chat.htmlclient .collaboration. enabled	CollaborationDebug	To enable or disable collaboration debugging.	Yes No	No

Changing the HTML Chat Client properties

You can change the HTML Chat Client properties to determine how frequently the ICM server polls the Customer HTML Chat Client, the servlet checks for polling problems, and the interval between an unsuccessful poll and the disconnection of the chat session.

To change the HTML Chat Client properties, modify the tenant website properties in the following table:

Property	Description	Possible values	Default/Recommended
chat.htmlclient.poll. interval	Indicates how often (in seconds) the server polls the Customer HTML Chat Client.	A number greater than zero.	8 seconds This value must be less than the check interval. Recommended: ● Maximum: 15 seconds ● Minimum: 5 seconds **Note:** A poll interval of less than 5 seconds can overload the ICM server.
chat.htmlclient.poll. checkinterval	Determines how often (in seconds) the servlet checks to notify the agent of any problem with Customer HTML Chat Client polling.	A number greater than zero.	20 This value must be less than the disconnect interval. Recommended: ● Maximum: 30

Property	Description	Possible values	Default/Recommended
chat.htmlclient.poll.disconnectinterval	Indicates the number of seconds before the servlet disconnects the chat session, if the Customer HTML Chat Client is unable to poll the server at least once within this interval.	A number greater than zero.	60 Recommended: ● Maximum: 120
chat.htmlclient.chatfail.message	Determines the message displayed to the Website when the customer tries to send a message, if the Customer HTML Chat Client loses connection with the Website.	Any text string.	[Agent did not receive your message]
chat.htmlclient.chaterror.message	Determines the message displayed to the customer, if the Customer HTML Chat Client loses connection with the Website.	Any text string.	[Chat connection error. Please disconnect this session]

Customizing the logo

By default, the Customer HTML Chat Client displays the Avaya logo. You can replace this with the logo of the contact center. Also, you can change the background color for the logo.

To customize the logo, modify the tenant website properties in the following table:

Property	Description	Possible values	Default
chat.htmlclient.logo.bgcolor	Background color for the logo.	English word or hex value	White (#FFFFFF)
chat.htmlclient.logo	Identifies the URL with the file name and path of the logo to display at the top of the Customer HTML Chat Client.	Any URL with a path and file name.	Images/avaya.gif The default value displays the Avaya logo. The image must be in a displayable format, such as GIF, JPG, or TIF.

Changing the window position and size

By default, the Customer HTML Chat Client opens as a frame docked in the main browser window of the Website customer. You can change how the Customer HTML Chat Client opens, where it opens in the customer browser, and the size of the Customer HTML Chat Client.

To change the window position and size, modify the tenant website properties in the following table:

Property	Description	Possible values	Default
chat.htmlclient.docked	Determines whether the Customer HTML Chat Client will open as a frame docked to the main browser window or a pop-up window.	True: Opens as a frame in the main browser window. False: Opens as a pop-up window.	True
chat.htmlclient.docked.proportion	If chat.htmlclient.docked is set to true, it determines the percentage of the chat client frame in proportion to the entire browser window.	A number less than or equal to 100	33 The chat client frame uses 33% of the browser window.
chat.htmlclient.docked.position	Indicates the position of the frame inside the browser window.	Left Right Top Bottom	Left
chat.htmlclient.undocked.location	If chat.htmlclient.docked is set to false, it indicates the starting location of the pop-up window.	Valid coordinates of the screen	0,0
chat.htmlclient.undocked.height	If chat.htmlclient.docked is set to false, it specifies the height of the pop-up window in pixels.	Any number	500
chat.htmlclient.undocked.width	If chat.htmlclient.docked is set to false, it specifies the width of the pop-up window in pixels.	Any number	400

Property	Description	Possible values	Default
Chat.htmlclient. undocked.title	If chat.htmlclient.docked is set to false, specifies the label text in the title bar of the pop-up window. **Note:** Avaya recommends a maximum of 64 characters in the title text. Some browsers will truncate a title of more than 64 characters.	Any text string	Avaya Customer Chat
Chat.htmlclient. undocked.timer	If chat.htmlclient.docked is set to false, it indicates the number of seconds before Avaya IC determines that the pop-up window failed to open. For example, a pop-up blocker prevents the Customer HTML Chat Client from opening.	Any number greater than zero.	30 Recommended: ● Minimum: 5

Changing the frame sizes

You can change the sizes of the different frames in the Customer HTML Chat Client.

To change the frame sizes, modify the tenant website properties in the following table:

Property	Description	Possible values	Default
chat.htmlclient. transcript.framesize	Specifies the height of the frame that displays the real-time chat transcript.	Any number greater than zero	* (asterisk)
chat.htmlclient. command.framesize	Specifies the height of the frame that contains the End Chat Session and Say buttons.	Any number greater than zero	55
chat.htmlclient. textentry.framesize	Specifies the height of the frame that displays the field where customers enter text for the chat.	Any number greater than zero	75
chat.htmlclient.logo. framesize	Specifies the height of the frame that contains the logo.	Any number greater than zero	80

Customizing the background colors

You can customize the background colors of the Customer HTML Chat Client to match the logo of the contact center, or meet Web standards for the contact center.

To customize the background colors, modify the tenant website properties in the following table:

Property	Description	Possible values	Default
chat.htmlclient. command.bgcolor	Specifies the background color of the frame that contains the command buttons.	English word or hex value	Blue (#335687)
chat.htmlclient. textentry.bgcolor	Specifies the background color for the text entry field.	English word or hex value	White (#FFFFFF)
chat.htmlclient. transcript.bgcolor	Specifies the background color for the transcript.	English word or hex value	White (#FFFFFF)

Customizing the text entry fields

You can customize the size and tooltip for the text entry field where the Website customer enters text into the Customer HTML Chat Client.

To customize the text entry fields, modify the tenant website properties in the following table:

Property	Description	Possible values	Default
chat.htmlclient. textentry.width	Determines the width of the text entry field in pixels.	Any number greater than zero	33
chat.htmlclient. textentry.size	Determines the number of lines visible in the text entry field.	Any number greater than zero	2
chat.htmlclient.entry. tooltip	Specifies the text that displays as a tooltip for the text entry field.	A text string	Enter chat message here

Customizing the welcome message

The Customer HTML Chat Client displays the welcome message to:

- The customer, when the customer requests a chat

- The agent, when the agent accepts the chat contact.

To customize the welcome message, modify the tenant website properties in the following table:

Property	Description	Possible values	Default
chat.htmlclient.welcome	The welcome message displayed to the customer and agent, when the agent joins a chat session.	Any text string	Welcome to Avaya Chat. You can chat and send pages.

Customizing the chat transcript

You can customize the appearance of the chat transcript displayed to the customer during a chat session. For example, you can customize the color and font for the text of:

- Agent comments
- Customer comments
- System messages

This section includes the following topics:

- Customizing common chat transcript properties on page 267.
- Customizing the chat transcript properties for agents on page 268.
- Customizing the chat transcript properties for customers on page 270.
- Customizing the chat transcript properties for the system on page 271.

Customizing common chat transcript properties

The common chat transcript properties determine the appearance of items that are common to all sections in the transcript.

To customize the common chat transcript properties, modify the tenant website properties in the following table:

Property	Description	Possible values	Default
chat.htmlclient.transcript.lineseparator	Defines the spacing between the consecutive lines.	Any valid HTML markup	

Property	Description	Possible values	Default
chat.htmlclient. transcript. nameseparator	Defines the spacing between the name and the transcript text.	Any valid text string or HTML markup	“: " A semi-colon and a space.
Chat.htmlclient. transcript. maxmessagesize	Specifies the maximum number of characters in a single text message typed by an agent or customer.	Any number from 1 to 4000.	1024

Customizing the chat transcript properties for agents

The chat transcript properties for agents determine the appearance of items in the chat transcript that relate to the participation of the agent in the chat session.

Note:
If the font value specified consists of more than one word, for example, Times Roman or Segoe UI, then such fonts must be specified within single quotes for them to appear correctly at the customer side during chatting.

To customize the chat transcript properties for agents, modify the tenant website properties in the following table:

Property	Description	Possible values	Default
chat.htmlclient.agent. name.font	Specifies the name of the font used to display the name of the agent in the transcript.	A font name	Times Roman
chat.htmlclient.agent. name.color	Specifies the color of the font used to display the name of the agent in the transcript.	English word or hex value	Blue (#335687)
chat.htmlclient.agent. name.size	Specifies the size of the font used to display the name of the agent in the transcript.	Any number	3
chat.htmlclient.agent. text.font	Specifies the name of the font used to display the messages typed by the agent.	A font name	Times Roman
chat.htmlclient.agent. text.color	Specifies the color of the font used to display the messages typed by the agent.	English word or hex value	Black
chat.htmlclient.agent. text.size	Specifies the size of the font used to display the messages typed by the agent.	Any number	3

Property	Description	Possible values	Default
chat.htmlclient.agent.link.font	Specifies the name of the font used to identify the hyperlinks in the messages typed by the agent.	A font name	Times Roman
chat.htmlclient.agent.link.color	Specifies the color of the font used to identify the hyperlinks in the messages typed by the agent.	English word or hex value	Blue (#335687)
chat.htmlclient.agent.link.size	Specifies the size of the font used to identify the hyperlinks in the messages typed by the agent.	Any number	3
chat.htmlclient.agent.name.pretag	Specifies the opening HTML tag used to customize the character style for the agent name.	The opening tag for an HTML character style, such as bold , italic , or underline <u>.	No default.
chat.htmlclient.agent.name.posttag	Specifies the closing HTML tag used to customize the character style for the agent name.	The closing tag for an HTML character style such as bold , italic , or underline </u>.	No default.
chat.htmlclient.agent.text.pretag	Specifies the opening HTML tag used to customize the character style for messages typed by the agent.	The opening tag for an HTML character style such as bold , italic , or underline <u>.	No default.
chat.htmlclient.agent.text.posttag	Specifies the closing HTML tag used to customize the character style for messages typed by the agent.	The closing tag for an HTML character style such as bold , italic , or underline </u>.	No default.

Customizing the chat transcript properties for customers

The chat transcript properties for customers determine the appearance of items in the chat transcript that relate to the participation of the customer in the chat session.

To customize the chat transcript properties for customers, modify the tenant website properties in the following table:

Property	Description	Possible values	Default
chat.htmlclient. customer.name.font	Specifies the name of the font used to display the name of the customer in the transcript.	A font name	Times Roman
chat.htmlclient. customer.name.color	Specifies the color of the font used to display the name of the customer in the transcript.	English word or hex value	Red
chat.htmlclient. customer.name.size	Specifies the size of the font used to display the name of the customer in the transcript.	Any number	3
chat.htmlclient. customer.text.font	Specifies the name of the font used to display the messages typed by the customer.	A font name	Times Roman
chat.htmlclient. customer.text.color	Specifies the color of the font used to display the messages typed by the customer.	English word or hex value	Black
chat.htmlclient. customer.text.size	Specifies the size of the font used to display the messages typed by the customer.	Any number	3
chat.htmlclient. customer.link.font	Specifies the name of the font used to identify the hyperlinks in the messages typed by the customer.	A font name	Times Roman
chat.htmlclient. customer.link.color	Specifies the color of the font used to identify the hyperlinks in the messages typed by the customer.	English word or hex value	Blue (#335687)
chat.htmlclient. customer.link.size	Specifies the size of the font used to identify the hyperlinks in the messages typed by the customer.	Any number	3

Property	Description	Possible values	Default
chat.htmlclient. customer.name.pretag	Specifies the opening HTML tag used to customize the character style for the customer name.	The opening tag for an HTML character style, such as bold , italic , or underline <u>.	No default.
chat.htmlclient. customer.name. posttag	Specifies the closing HTML tag used to customize the character style for the customer name.	The closing tag for an HTML character style such as bold , italic , or underline </u>.	No default.
chat.htmlclient. customer.text.pretag	Specifies the opening HTML tag used to customize the character style for messages typed by the customer.	The opening tag for an HTML character style such as bold , italic , or underline <u>.	No default.
chat.htmlclient. customer.text.posttag	Specifies the closing HTML tag used to customize the character style for messages typed by the customer.	The closing tag for an HTML character style such as bold , italic , or underline </u>.	No default.

Customizing the chat transcript properties for the system

The chat transcript properties for system determine the appearance of items in the chat transcript that relate to system messages in the chat session. System messages identify events such as the connection of the agent to the chat session.

To customize the chat transcript properties for system, modify the tenant website properties in the following table:

Property	Description	Possible values	Default
chat.htmlclient.system. name	Identifies the word that denotes messages from the system, such as, “System: Connection Established.”	A text string	System
chat.htmlclient.system. name.font	Specifies the name of the font used to display the system name in the transcript.	A font name	Times Roman

Property	Description	Possible values	Default
chat.htmlclient.system.name.color	Specifies the color of the font used to display the system name in the transcript.	English word or hex value	Blue (#335687)
chat.htmlclient.system.name.size	Specifies the size of the font used to display the system name in the transcript.	Any number	3
chat.htmlclient.system.text.font	Specifies the name of the font used to display the system messages.	A font name	Times Roman
chat.htmlclient.system.text.color	Specifies the color of the font used to display the system messages.	English word or hex value	Black
chat.htmlclient.system.text.size	Specifies the size of the font used to display the system messages.	Any number	3
chat.htmlclient.system.link.font	Specifies the name of the font used to identify the hyperlinks in the system messages.	A font name	Times Roman
chat.htmlclient.system.link.color	Specifies the color of the font used to identify the hyperlinks in the system messages.	English word or hex value	Blue (#335687)
chat.htmlclient.system.link.size	Specifies the size of the font used to identify the hyperlinks in the system messages.	Any number	3
chat.htmlclient.system.name.pretag	Specifies the opening HTML tag used to customize the character style for the system name.	The opening tag for an HTML character style, such as bold , italic , or underline <u>.	No default.
chat.htmlclient.system.name.posttag	Specifies the closing HTML tag used to customize the character style for the system name.	The closing tag for an HTML character style such as bold , italic , or underline </u>.	No default.

Property	Description	Possible values	Default
chat.htmlclient.system.text.pretag	Specifies the opening HTML tag used to customize the character style for system messages.	The opening tag for an HTML character style such as bold , italic , or underline <u>.	No default.
chat.htmlclient.system.text.posttag	Specifies the closing HTML tag used to customize the character style for system messages.	The closing tag for an HTML character style such as bold , italic , or underline </u>.	No default.

Customizing the timestamp on chat transcripts

By default, chat transcripts sent to Website customers do not include a timestamp. You can customize the Customer HTML Chat Client to include a timestamp on the transcript and specify the format for that timestamp.

To customize the timestamp, modify the tenant website properties in the following table:

Property	Description	Possible values	Default
chat.htmlclient.timestamps.enabled	Indicates whether chat transcripts will include a timestamp. By default, there is no timestamp.	False True	False
chat.htmlclient.timestamps.showdate	Indicates whether the timestamp will include the date. By default, the timestamp does not include the date.	False True	False

Property	Description	Possible values	Default
chat.htmlclient.timestamps.format	Determines the format of the timestamp. The available formats are based on the locale selected for the chat session. The machine used by the Website customer determines the time that is displayed. The following examples are based on a US locale and assume that you set chat.htmlclient.showdate to true. The format may be different if the customer is in a different locale.	Short: 9/20/04 2:15pm Medium: 20 Sep, 2004 2:15:50 PM Long: 20 September, 2004 2:15:50 PM EST	Medium
chat.htmlclient.timestamps.prefix	Determines the opening string that encloses the timestamp. It is only used, if timestamp is enabled.	A string of any length or an empty string.	The open bracket character: “[“
chat.htmlclient.timestamps.postfix	Determines the closing string that encloses the timestamp. It is only used, if timestamp is enabled.	A string of any length or an empty string.	The close bracket character: “]“

Customizing the tooltips

You can customize the tooltips for the text entry field where the Website customer enters text into the Customer HTML Chat Client.

To customize the text entry fields, modify the tenant website properties in the following table:

Property	Description	Possible values	Default
chat.htmlclient.button.saytext.tooltip	Specifies the text that displays as a tooltip for the Send Message button.	A text string	Send Message
chat.htmlclient.button.close.tooltip	Specifies the text that displays as a tooltip for the Close button.	A text string	Close Chat Window
chat.htmlclient.button.end.tooltip	Specifies the text that displays as a tooltip for the End Chat Session button.	A text string	End Chat Session

Property	Description	Possible values	Default
chat.htmlclient.button.help.tooltip	Specifies the text that displays as a tooltip for the Help button.	A text string	Help
chat.htmlclient.entry.tooltip	Specifies the text that displays as a tooltip for the text entry field.	A text string	Enter chat message here

Adding a help file

By default, the Customer HTML Chat Client does not include a help file. You can add a link to an HTML page that is displayed to the Website customer, when the customer selects the Help button. The Help button is not visible to the customer unless you configure the Customer HTML Chat Client for the help file.

This section includes the following topics:

- Guidelines for the Customer HTML Chat Client help file on page 275.
- Recommended content for the Customer HTML Chat Client help file on page 275.
- Making the Help button visible on page 276.

Guidelines for the Customer HTML Chat Client help file

Any help file for the Customer HTML Chat Client meets the following guidelines:

Host the help file on the Avaya IC Website: The Customer HTML Chat Client does not download the help file to the customer. Avaya recommends that you host the help file on the Avaya IC Website.

Design the help system to use HTML pages: When you enable the Help button, you provide the URL and path to an HTML page. You can design this HTML page as a set of links to other HTML pages, or to include all of the information that you want the Website customer to see.

Avoid compiled help systems: Do not use a compiled help system, such as WinHelp or Microsoft HTML Help (CHM). Compiled help systems require the Windows executable. Customers who use other operating systems will not be able to access these help systems.

Recommended content for the Customer HTML Chat Client help file

Avaya recommends that, at a minimum, the Customer HTML Chat Client help file includes the following contents:

- Supported browsers for Website customers, as described in Supported Web browsers for Website customers on page 256.

- Troubleshooting information for problems that customers are likely to encounter, such as pop-up blockers, as described Troubleshooting the Website Multi-Tenant Administration pages on page 285.

Making the Help button visible

To make the Help button visible on the Customer HTML Chat Client, modify the tenant website property in the following table:

Property	Description	Possible values	Default
chat.htmlclient.helpurl	When you add a value to this property: ● Make the Help button visible. ● Identify the URL with the file name and path of the HTML file that will be displayed when the Website customer selects the Help button.	Any URL with a path and file name.	empty

Enabling the debug window

Important:
Do not enable the debug window in a production environment. Use the debug window in a development environment to identify problems.

To enable the debug window, modify the tenant website property in the following table:

Property	Description	Possible values	Default
chat.htmlclient.debug.enabled	Turns debugging on or off.	True False	False Debug is turned off.

Disabling the Enter event

Some languages, for example Japanese, use the **Enter** key to select characters. The Customer HTML Chat Client might respond to the Enter event and send the message prematurely. When this feature is turned off, you must click on the **Send** button to send a chat.

To turn off the default send operation when the **Enter** key is pressed:

1. Go to IC Web Management Administration web pages.
2. Select **MultiTenant Administration**.
3. Select **Tenant Properties**.
4. Select your tenant.
5. Select **Language**.
6. Select **Chat**.
7. Look for **chat.htmlclient.entry.sendonenter**.
8. Change the value to **0**.
9. Select the **Update Data** button at the bottom of the page.

Emoticons

Emoticons are the iconic representation of the facial expressions, such as smiley, sad, tired, and so on.

You can use the `emoticons.properties` file to configure emoticons. In properties files, you can add new emoticons or update existing. You have to link an image to a sequence of characters.

Note:

If the sequence of characters contains a special character then you have to precede each special character with escape character (`\`). For example, consider the character sequence `x\-\)`. In this example all the special characters except `x` are preceded with the \.

The `emoticons.properties` file is located at: `AVAYA-IC-HOME/comp/icm`

You can enter the configured sequence of characters in the message area of chat application and the related image is displayed in the transcript area of all the parties involved in the conversation.

The following table lists the default emoticons and their character sequence that you have to enter in the message area of the chat application:

Emoticons	Character Sequence	Facial Expression
	?-|	Ponder
	:(or :-<	Sad
	:)	Smile

Emoticons	Character Sequence	Facial Expression
	:@	angry
	:o	surprised
	:|	disappointed
	:U	thankyou
	(Y)	thumbsup
	:8	holdon

For Website, the images of emoticons are stored in the following folder: `Avaya-IC-HOME\comp\website\public\htmlclient\images\emoticons`.

Configuring Avaya IC Manager to enable emoticons

Before you can actually start using emoticons, you have to configure emoticons through Avaya Avaya IC Manager.

To configure emoticons in Avaya IC Manager:

1. In the Avaya IC Manager window, click the **Configuration** tab.
2. In the left pane, select **Chat** > **ICM**.
3. On the toolbar, click **New**.
4. Enter the value in the **Global ICM Name** and **ICM Server Name** fields.
5. Select the **Enable Emoticons** check box.
6. Click **OK**.

Note:
You must restart the ICM service to reload the changed properties in the Avaya IC Manager of ICM.

Chat typing status

The chat typing status is a message that the chat client window displays at the bottom side.

The chat typing status in the chat client window at the customer's end indicates that the agent is now typing a message. Similarly, the chat typing status in the chat client window at the agent's end indicates that the customer is now typing a message.

The chat client window displays the typing status for a specific threshold time, which you can configure in Avaya IC Manager. If there is no typing activity in the chat client for the configured threshold time, the system removes the chat typing status from the chat client window.

You can configure IC Manager to enable the chat client to display the chat typing status. You can enable the chat typing status for an individual agent, a group, or a tenant.

To enable the chat typing status in the Avaya Agent Web Client:

1. In the Avaya IC Manager window, click the **Agent** tab.
2. In IC Manager, from the main menu, select **Tools** > **Groups**.

   The system displays the **Group Manager** dialog box.
3. In the left pane, select a group, a tenant, or an agent from a group, for which you want to enable the chat typing status.
4. In the **Sections** field, select the **Agent/Desktop/Chat/Application** section.
5. In the right pane, click **Create New Setting** on the **Settings** toolbar.

   The system displays the **Assign Property** dialog box.
6. Click the **Property** field and select the **ShowTypingStatus** property.
7. Click the **Property Value** field and select **Yes**.
8. Click the **Descendants May Override** check box if you want to allow the descendants of the selected group to change the configuration.
9. Click **OK**.

   The system adds the selected property in the list.
10. In the right pane, click **Create New Setting** on the **Settings** toolbar.
11. Click the **Property** field and select the **TypingStatusThreshold** property.
12. Click the **Property Value** field and enter the threshold time in seconds.

    The system displays the chat typing status in the Chat window for the time that you specify in the **TypingStatusThreshold** property.

    If you do not add the **TypingStatusThreshold** property, the system displays the chat typing status for the default time, 12 seconds.
13. Click the **Descendants May Override** check box if you want to allow the descendants of the selected group to change the configuration.
14. Click **OK**.

    The system adds the selected property in the list.
15. In the **Group Manager** window, click **OK**.

To enable the chat typing status in Web Agent:

1. Go to the `<AARC install_dir>\Webagent\` directory.
2. Open the `Application.properties` file to edit.
3. Set the `chat.typingstatus.enable` property value to true.
4. Set the `chat.typingstatus.messagetimeout` property value to 12 seconds.
5. Save the `Application.properties` file.

Note:
For displaying the chat typing status in a localized language, set the localized typing status string in the `chat.typingstatus.statusmessage` property, in the `ClientMessages_<lang>.properties` file.

Note:
If Web Agent does not display the updated chat typing message, you must restart Web Agent.

To enable the chat typing status at the customer end:

1. In a Web browser, navigate to the IC Website administration page.

   `http://<server_name>/website/admin/login.jsp`.
2. Enter the user name and password and click **Next** to login to the IC Website administration page.
3. Access the add metadata page.

   `http://<server_name>/website/admin/tenancy/addmd.jsp`
4. Add the following metadata property:
   - Metadata name = chat.htmlclient.typingstatusmsg
   - Default value = typing
   - Select the Tenant Property option
5. Click **Add Metadata**.
6. Add the following metadata property:
   - Metadata name = chat.htmlclient.typingstatusenable
   - Default value = true
   - Select the **Tenant Property** option
7. Click **Add Metadata**.
8. Add the following metadata property:
   - Metadata name = chat.htmlclient.typingmsgtimeout
   - Default value = 12 (in seconds)
   - Select the **Tenant Property** option
9. Close the browser.

Note:
If HTML Chat client window does display the updated chat typing message, you must restart the Web site.

Configuring blind chat transfer

You can configure IC Manager to enable blind transfer.

To add the AllowBlindTransfer property:

1. In IC Manager, from the main menu, select **Tools** > **Property Declarations.**
2. In the **Property Declarations** dialog box, in the **Property Selection** section, click **Agent/ Desktop/WAC**.
3. In the right pane, under **Props for Agent/Desktop/WAC**, click **New**.
4. On the **Declare Property** dialog box, enter the following information:
   - **Name**: AllowBlindTransfer
   - **Description**: AllowBlindTransfer
   - **Property DataType**: interger
5. Click **OK**.

   The system adds the property to the **Props for Agent/Desktop/WAC** list.
6. Click **OK**.

To enable blind transfer in the Avaya Agent Rich Client:

1. In IC Manager, from the main menu, select **Tools** > **Groups**.

   The system displays the **Group Manager** dialog box.
2. In the left pane, select a group or a tenant for which you want to enable blind transfer.
3. In the **Sections** field, select the **Agent/Desktop/WAC** section.
4. Click the **Property** field and select the **AllowBlindTransfer** property.
5. Click the **Property Value** field and enter `1`, `2`, or `3`.

   Specify whether agents perform a consulative transfer or a blind transfer or both. The values you can set are:
   - `1` - Agents can perform consultative transfer only.
   - `2` - Agents can perform blind transfers to queues only.
   - `3` - Agents can perform both blind transfers and consultative transfers.
6. Click **Apply**.

7. Click **OK**.

   The system adds the selected property in the list.

8. In the **Group Manager** window, click **OK**.

Example: Changing the images for a button

The Customer HTML Chat Client uses four different images to emulate each button. These button images indicate the following states:

- Pressed
- Grayed or unavailable
- Selected
- Normal

In this example, the image on the Say button needs to be replaced. To replace the Say button image, you need to replace all four of the button images. Each of the replacement images need to emulate the state that the image represents.

To replace the Say button:

1. Create copies of the four Say button images and place them in a backup directory.

   Avaya IC installs the button images in the following directory on the Website system: `IC_INSTALL_DIR\etc\comp\website\public\htmlclient\images`

2. Create **.gif** images with the new button image for the Say button to replace the images described in the following table. If you have only one image and you want this image to represent all four button states, you must create four versions of the button image.

Image file name	Button state
buttonsay01.gif	Normal
buttonsay02.gif	Selected
buttonsay03.gif	Grayed
buttonsay04.gif	Pressed

3. Save the custom Say button images in the following directory on the Website machine: `IC_INSTALL_DIR\etc\comp\website\public\htmlclient\images`
4. Test the Customer HTML Chat Client with the custom Say button images.

Localization properties

All text in the Customer HTML Chat Client is in English. You can modify some of the website tenant properties to translate the text into another language.

The following table describes the website tenant properties that modify localizable text fields. All of these properties are described in more detail in Customizing tenant website properties on page 256.

Property	Text
chat.htmlclient.chatfail.message	[Agent did not receive your message]
chat.htmlclient.chaterror.message	[Chat connection error. Please disconnect this session]
chat.htmlclient.button.saytext.tooltip	Send Message
chat.htmlclient.button.close.tooltip	Close Chat Window
chat.htmlclient.button.end.tooltip	End Chat Session
chat.htmlclient.button.help.tooltip	Help
chat.htmlclient.entry.tooltip	Type your message here
chat.htmlclient.welcome	Welcome to Avaya Chat. You can chat and send pages
chat.htmlclient.undocked.title	Avaya Customer Chat
chat.htmlclient.system.name	System

Chat Timestamp feature

When an agent is handling a chat contact no timestamp is shown with the chat messages, however the old website (After enabling the timestamp property from the admin site) and csportal does show the timestamp for each chat message at customer end.

Using the Chat Timestamp feature the chat messages shown at the agent application will also contain the timestamp when enabled on the ICM server configuration.

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

Note:

1. The timestamp is not shown with the system phrases such as "caller type, transfer/ Conference phrases, supervisor entering/leaving the chat room phrases"
2. The timestamp shown at the customer end "website/csportal" are not using the ICM utc time. The Website/CSPortal components use their own time. If there is no time-sync there could be a possibility that the agent or customer timestamp shown are different. You must have time-sync between the systems.

Importing the SC.xml file

You must import the sc.xml file to get the Enable Timestamp option in the ICM Configuration.

1. Login to the IC Manager application.
2. In the IC Manager window, click **Manager** > **Options**.
3. In the **Options** window, click the **Environment** tab.
4. In the **Environment** tab, click **Import Configuration...**.
5. In the **Open** window, goto **<Install_Path>IC73\etc** folder.
6. In the **etc** folder select **sc.xml** file and click **Open**.
7. In the **Validate sc.xml** window, click **OK**.
8. In the **Options** window, click **OK**.
9. In the **IC Manager**, click **Manage** > **Refresh**.
10. Close the **IC Manager**.
11. Open the **IC Manager**.

Enabling the TimeStamp feature

To enable Timestamp feature:

1. Login to the IC Manager application.
2. In the **IC Manager** window, click the **Configuration** tab.
3. In the left pane, goto **Tables** > **Chat** > **ICM** > **ICM DS Record**.

   Note:
   If you do not already have the ICM DS Record, then you must click New and create a ICM DS Record.

4. Click to select the **Enable Timestamps** option.

5. Click **Apply**.
6. Restart the Avaya IC ICM service.
   a. Login to the Core Server system.
   b. Click **Start** > **Run**.
   c. In the **Run** window, type **services.msc** and press **Enter**.
   d. In the **Services** window, right-click **Avaya IC ICM Service 7.3** and select **Restart**.

Note:
Out of the Box, the timestamp feature on the agent application is disabled. The Enable Agent Timestamps option is not selected. The administrator has to manually enable this feature to use the agent side timestamp feature. Do not enable the Timestamp feature if you are your network contains new agent application and old agent application. This feature only works on Agent applications from IC 7.3.3 onwards.

Troubleshooting the Website Multi-Tenant Administration pages

Problem: If you try to change the default language for a chat tenant, the Invalid Language error message is displayed.

Solution: Execute the following steps to resolve this issue:

1. On the **IC Website Multi-Tenant Administration** page, click the **Enable Languages** link in the left pane.
2. In the right pane, select the desired tenant from the **Select a tenant** drop-down list and click **Customize Tenant Languages**.
3. Select another language by selecting the option in the **Default** column.

   For example, if English and French are the languages defined for the Tenant with default language English, Select **French** as the default language.
4. In the **Display Text** column, enter the value for **English** language.
5. Click the **Edit Languages** button.
6. Now, select **English** as the default language again by selecting the option in the **Default** column.
7. Click the **Edit Languages** button.

Troubleshooting the Customer HTML Chat Client

This section describes some common problems that can occur with the Customer HTML Chat Client and the solutions for these problems.

This section includes the following topics:

- Frame killer in pushed Web page unloads chat session on page 286
- Customer HTML Chat Client does not open in pop-up window on page 287
- Customer requests chat transcript after session closed on page 287

Tip:
If you encounter an issue not in the documentation, contact Avaya CRM Technical Support.

Frame killer in pushed Web page unloads chat session

Problem: An agent pushes a Web Page to a customer. The Web Page includes a frame killer. As a result of the frame killer, the chat session is unloaded, and the customer and cannot communicate.

Solution for Web page: If the Web Page that the agent pushes includes code for a frame killer, the Web page cannot be displayed in the frameset for the Customer HTML Chat Client.

Solution for Website customer: The customer can re-enter the chat session after a chat session is unloaded. To re-enter the chat session, the customer clicks the **Back** button on the Web browser.

Solution for agent: Wait until the customer re-enters the chat session. The Customer HTML Chat Client displays a reconnect message in the transcript when the customer re-enters. Do not Push the same URL to the customer.

Tip:
To configure the length of time within which a customer can re-enter a chat session, see Changing the HTML Chat Client properties on page 262.

Customer HTML Chat Client does not open in pop-up window

Problem: Customer requests a chat session with an agent, but the Customer HTML Chat Client does not open in a pop-up window. This problem usually occurs because the customer uses a pop-up blocker. This problem only occurs with the undocked mode, whether the Customer HTML Chat Client opens in a separate, pop-up window.

Solution for customer: Check whether pop-up blocker is enabled. If the pop-up blocker, is enabled, disable the pop-up blocker and restart the chat session.

Solution for Customer HTML Chat Client: Configure the Customer HTML Chat Client to open as a frame docked in the main browser window of the Website customer if the pop-up window is blocked. For more information, see Changing the window position and size on page 264.

Customer requests chat transcript after session closed

Problem: After the agent and customer disconnect from the chat session, and the chat session is closed, the customer requests a copy of the chat transcript.

Solution: When the customer first requests a chat session, the customer must select the option to have an email transcript mailed and provide an email address. An agent cannot send a copy of the chat transcript after the chat session starts.

Chapter 12: Advanced agent settings

This section describes how you would customize the agent environment for the Avaya Agent desktop application.

> **Important:**
> For information on customizing Avaya Agent Web Client, see *Avaya Agent Web Client Customization*.

This section includes the following topics:

- Setting up the home directory and working directory on page 288
- Configuring UNC to UNIX path mapping on page 293
- Using a shared directory for agent files on page 295
- Customizing the Web Agent on page 299
- Configuring RONA for the chat channel on page 301
- Configuring RONA for the email channel on page 304
- Creating wrap up, AuxWork, and Logout codes on page 308
- Audio and visual notifications for the chat channel on page 315
- Customizing the window for the popped out chat tab on page 318

For information about adding, modifying, and deleting agents, see Using the Agent Manager on page 215.

Setting up the home directory and working directory

Avaya Agent and Avaya Agent Web Client use different agent properties to specify the directory that stores the global resources shared by agents and agent settings, such as agent resources, email drafts, and task data.

This section includes the following topics that are designed to help you determine how to set these directory properties:

- Directory properties for agent applications on page 289.
- Purpose of the directory properties on page 289.
- Recommended deployments for the home directory and working directory on page 290.
- Configuring the home directory on page 291.

- Configuring the working directory on page 292.

Directory properties for agent applications

The following table shows the directory properties for Avaya Agent and Avaya Agent Web Client.

Application	Directory type	Property section.name
Avaya Agent	Home directory	Agent/Desktop/WAC.HomeDir **Note:** After you set the home directory for Avaya Agent, you must copy the following directories located in the `IC_INSTALL_DIR\WebAgent` directory to the shared directory: • lexicons • images • Editlive After copying the above directories, ensure that the directories have read, write and execute permissions. In IC 7.3.2 FP, Editlive! 9.0.0.98 is supported.
Avaya Agent Web Client	Working directory	Agent/Desktop/WebClient.WorkingDirectory

Purpose of the directory properties

Although Avaya Agent and Avaya Agent Web Client give different names to the shared directory, the structure and content of the home directory and working directory is identical. Both of these directories work as a shared directory that stores:

- Global resources shared by Avaya IC agents
- Settings for individual agents, such as agent resources, email drafts, and task data

For Avaya Agent Web Client in an environment with multiple machines that host WebConnector, the working directory ensures that an agent always has access to the correct agent settings. When the working directory is correctly configured in a shared directory, Avaya Agent Web Client can route the agent login to any WebConnector machine and access the task data and resources for that agent.

Recommended deployments for the home directory and working directory

How you set up the home directory and working directory depends upon the deployment of the Avaya IC system and how the agents share global resources. For example, you can:

- Create one shared directory for all agents in a system, whether those agents use Avaya Agent or Avaya Agent Web Client.
- Create more than one shared directory to give agents access to different sets of global resources.

This section includes the following topics that describe the recommended settings for the most common Avaya IC deployments:

- Deployment with one shared directory for all agent resources on page 290.
- Deployment with several shared directories for different sets of agent resources on page 290.
- Deployment for a clustered WebConnector environment on page 291

Deployment with one shared directory for all agent resources

In this deployment, all Avaya IC agents need access to all global resources. You must create one shared directory in a location that all agents can access.

The shared directory serves as the home directory for Avaya Agent and the working directory for Avaya Agent Web Client. The values for the home directory property and the working directory property all point to the same shared directory.

Set the value of the following properties as the value of the shared directory location at the IC node level:

- `Agent/Desktop/WAC.HomeDir` property for Avaya Agent
- `Agent/Desktop/WebClient.WorkingDirectory` for Avaya Agent Web Client

Deployment with several shared directories for different sets of agent resources

In this deployment, different agent workgroups need access to different sets of global resources. Avaya recommends that you create a different shared directory for each set of global resources. Agents can only belong to workgroups that have the same shared directory.

Whether one shared directory serves as the home directory for Avaya Agent and the working directory for Avaya Agent Web Client depends upon how you set up the agent workgroups. If an agent workgroup includes agents who work in Avaya Agent and in Avaya Agent Web Client, then the values for the home directory property and the working directory property must point to the same shared directory.

Note:
With this deployment, if some global resources are in more than one location and an agent updates a global resource, you must manually copy that updated resource to the other location.

Set the value of the following properties as the value of the shared directory location at the workgroup level:

- `Agent/Desktop/WAC.HomeDir` property for Avaya Agent
- `Agent/Desktop/WebClient.WorkingDirectory` for Avaya Agent Web Client

Deployment for a clustered WebConnector environment

For a clustered WebConnector environment, you must:

- Configure the Working Directory to point to a shared location.
- Make sure that the shared location is accessible to all agents.

Configuring the home directory

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 machine that hosts Avaya Agent accesses 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 machine.

Note:
Even if the home directory uses the same shared directory as the working directory, possibly you need to use a different syntax to configure the home directory property.

To configure the home directory:

1. Create the shared directory for the home directory on a network machine, if it does not already exist.
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 IC Installation and Configuration.

   The following table provides examples of the syntax used to configure the home directory property. These examples use the `AgentResource` directory on a machine 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 machine. **Note:** Do not use this syntax if the shared directory is on a UNIX machine.	`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 machine. For more information about UNC mapping, see Configuring UNC to UNIX path mapping on page 293.	`\\resource.xyzcorp.com\AgentResource`

Configuring the working directory

The working directory property is always configured from the perspective of WebConnector. The syntax that you use to configure the working directory property depends upon the operating system of the machine that hosts WebConnector for Avaya Agent Web Client and how that machine will access the shared directory.

Note:
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.

To configure the working directory:

1. Create the shared directory for the working directory on a network machine, if it does not already exist.
2. Ensure that all machines that host WebConnector for Avaya Agent Web Client:
   - Can access the shared directory for the working directory through one of the following methods:
     - For a Windows machine: a mapped drive or UNC notation in Windows Explorer
     - For a UNIX machine, an NFS mount or samba shares 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 IC Installation and Configuration.

   The following table provides examples of the syntax used to configure the working directory property. These examples use the `AgentResource` directory on a machine named `resource.xyzcorp.com` as the shared directory.

WebConnector access to shared directory	Syntax for working directory
You map the Z: drive on the WebConnector machine to the shared directory folder hosted on a Windows network machine. **Note:** Do not use this syntax, if WebConnector is on a UNIX machine.	`Z:\AgentResource`
The WebConnector machine uses UNC notation in Windows Explorer to access the shared directory. **Note:** Do not use this syntax, if WebConnector is on a UNIX machine.	`\\resource.xyzcorp.com\AgentResource`
You perform an NFS mount for the shared directory on the WebConnector machine. **Note:** Do not use this syntax, if WebConnector is on a Windows machine.	/opt/AgentResource

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 WebConnector uses to access the folder.

Tip:
You do not need to map the working directory for the WebConnector application server. However, you can map this directory if desired.

This section includes the following topics:

- Prerequisites for UNC to UNIX path mapping on page 294.
- Requirements for entries in the UNC to UNIX Path Mapping field on page 294.
- Accessing multiple folders on one machine on page 294.
- Examples of entries in the UNC to UNIX Path Mapping field on page 295.

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 machine that hosts the attachments directory to make the folders and files accessible from a Windows machine.
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 desired.
   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 machine. The Java Application Bridge only considers the first entry for a given machine in the table. All subsequent entries are ignored.
- You can only use the format **`\\`*`machine_name`*** in the **UNC Machine Name** column.
- You can only use valid UNIX paths in the **UNIX Path** column.

Accessing multiple folders on one machine: You cannot add multiple entries for a machine in the UNC to UNIX Path Mapping field. If you want to store files for attachments in multiple folders on the same machine:

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 Machine Name** column, enter the name of the machine 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 the 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 Machine Name	**UNIX Path**	
\\sunbox1	/opt/data/attachments	A valid entry in both the columns.
\\sunbox2\	/opt/data/attachments	An invalid entry in the **UNC Machine Name** column. The Java Application Bridge cannot accept an entry that ends with a backslash.
\\sunbox1	/opt/data	Entry will be ignored as there is already an entry for this UNC machine name.
\\sunbox3	/	A valid entry in both columns. The **UNIX Path** entry points to the root directory on the machine.
\\sunbox4		An invalid entry in the UNIX Path column. For root directory, enter /, as shown in the above entry.

Using a shared directory for agent files

By default, agent resources, preferences, email drafts, and log files are not shared. Instead, Web Agent stores these files in the Web Agent installation directory. This means that if you want to change the resources for all agents, you need to change the resource file on each agent's machine. It also means that agents must log into the same machine every day to make sure that they have the same resource and preference settings.

You can eliminate these potential problems by setting up a shared network directory for Web Agent files. You can then administer the files from a single location, and agents can log in to any machine and have the same resources and settings available to them.

Setting up a shared directory

To set up a shared directory:

1. Select a suitable shared network location. For example: `\\Avaya\chatserver\CommonAgentFiles`
2. Set the Share permissions on this directory so that agents have Read and Write access.
3. In Avaya IC Manager, set the following properties depending on your agent application:

- If your agents use Avaya Agent desktop, set the `Agent/Desktop/WAC/HomeDir` property to point to the directory you created in step 1. You can use a UNC path or a mapped network drive.
- If your agents use Avaya Agent Web Client, set the `Agent/Desktop/WebClient.WorkingDirectory` property to point to the directory you created in step 1. This directory must be accessible from the server running the Avaya Agent Web Client application. You can use a UNC path or a mapped network drive.

Important:
If your contact center uses a mix of Avaya Agent Web Client and Avaya Agent desktop applications, the `Agent/Desktop/WebClient.WorkingDirectory` and `Agent/Desktop/WAC.HomeDir` should point to the same location. Avaya Agent Web Client accesses the files through the Web Application Server.

For more information about the home directory and the working directory, see Setting up the home directory and working directory on page 288, Changing property settings on page 373, and Agent property descriptions on page 574.

Default files and directories created

When the Web Agent is started for the first time, several default files and directories are created:

- Application.properties

  A global level configuration file. For more information, see Customizing the Web Agent on page 299.

- GlobalPreferences.xml

  The `Globalpreferences.xml` file is intended to be used on a shared network drive to set preferences globally for all the agents without making changes on each individual agent system. However, agents can override global preferences by setting their own preferences through Web Agent. The preferences that agent sets through Web Agent are stored in the `agentpreferences.xml` file.

  The preferences in the `globalpreferences.xml` file are considered as the default preferences. However, if there is an `agentpreferences.xml` file with different preferences, the preferences in the `agentpreferences.xml` file overrides the preferences in the `globalpreferences.xml` file.

  Additionally, the `globalpreferences.xml` file is used to create the `agentpreferences.xml` file when new agents first log in to the system.

  Configuring the `globalpreferences.xml` file:

  1. Put the `globalpreferences.xml` file on a shared network drive.
  2. Log in to Avaya IC Manager.
  3. In IC Manager, from the main menu, select **Tools** > **Property Declarations**.

     The system displays the **Property Declarations** window.

4. In the **Property Selection** field, select the `Agent\Desktop\WAC` property.
5. In the **Props for Agent/Desktop/WAC** field, select the `HomeDir` property.
6. Set the `HomeDir` property value to the shared network path where you put the `globalpreferences.xml` file.
   a. Click the **Values** tab at the bottom of the **Property Declarations** window.
   b. On the **Values** tab, click **New** to add a new value.
   c. In the **Name** field, enter the shared network path.
   d. In the **Description** field, enter the description for the specified path.
   e. Click **OK**.
7. Click **OK**.

- GlobalResources.xml

  Resources created for use by all agents that point to the shared drive.
- Agents directory

  A directory will be created under this for each agent that uses this HomeDir value. Within that directory, the files discussed in Using a shared directory for agent user documents on page 297 are stored.
- Lexicons.
- Logs.

  This directory will contain a subdirectory for each workstation from which an agent logs on. Within that directory `webagent` log file is stored, if tracing is turned on.The subdirectory is the machine name of each workstation. Because agents can log in from any workstations, the log files are saved by workstation ID. The name of the agent who is logging in is included in the log file information.

Using a shared directory for agent user documents

The following table describes the agent-specific files:

File name	Description
AgentResources.xml	Agent specific resources

File name	Description
AgentPreferences.xml	Contains values set via the Tools, Preferences tab of the Web Agent. AgentPreferences.xml is accessed by Avaya Agent, but not by Avaya Agent Web Client. Avaya Agent Web Client stores similar information as properties in the IC database.
AgentEmailDrafts.xml	Draft responses of emails.

These files can be accessed by the Avaya Agent desktop and the Avaya Agent Web Client. Any changes to the user information is automatically saved under the agent's user name when the agent logs out. Maintaining agents' user documents at a network location is useful in situations where agents can be assigned to different machines on different days, or where two or more agents may share the same machine.

Web Management automatically creates a subdirectory on the shared directory for each agent account and saves the agent's user document within that subdirectory. This lets the agent set preferences and add new resources at one workstation on Monday, and then log in to those same preferences and resources at a different workstation on Tuesday. It also allows two agents on the same machine to maintain separate preferences and resources.

Creating shared resources for agents

You can create resources agents can use when they are interacting with customers. A resource can be a text message, a URL, or an email. Email resources can include **cc** and **subject** header fields, and can contain file attachments.

Global Resources are accessed by both Avaya Agent desktop and Avaya Agent Web Client, but only Avaya Agent desktop can create global resources. Global resources are created by a supervisor or administrator through the Web Agent, in the same manner that agent resources are created. They are saved in the GlobalResources.xml file. See *Avaya Agent User Guide* for information on creating resources.

If an agent has problems with shared resources, verify the following events have not occurred:

1. Working directory is not set, default is set to `IC_INSTALL_DIR/etc/workingdir`.

   All agent resources are created under this directory, if the administrator later changes the property then the agents are responsible for moving the resource files.

2. Working directory is set but not accessible temporarily when the agent logs in.

   If the agent had any resources created when this directory was accessible, then those resources are not visible in this session. The agent should not create any resources in this session since these are stored in a temporary location (defaulted to `IC_INSTALL_DIR/etc/workingdir`). Any resource created in this session would not be available when the original working directory becomes accessible.

Customizing the Web Agent

You can modify certain aspects of the Web Agent interface, including the layout of the toolbar and menus, the look of the agent client, logging level for troubleshooting, and fonts. These modifications are made in the Web Agent interface, in configuration files, or in Avaya IC Manager, depending on the type of modification.

This section only applies to the Avaya Agent desktop, for information about customizing Avaya Agent Web Client, see *Avaya Agent Web Client Customization*.

Web Agent interface

You can set chat, email, and font size preferences for each agent through the Web Agent interface. For more information, see the *Avaya Agent User Guide*.

Configuration files

Some customizations can be made on a per agent, tenant, or workgroup basis using a configuration file. This functionality is mainly used to set logging parameters.

The configuration file `application.properties` is saved in the directory specified in the `HomeDir` property of the `Agent/Desktop/WAC` subsection in Avaya IC Manager. Because `HomeDir` can be set on a global, tenant, or workgroup basis, the options set in the `application.properties` file can be applied at any of those levels. If a file is configured at all three levels, the lowest level will be used (global is the highest level, workgroup is the lowest). For more information, see Agent/Desktop/WAC properties on page 622.

Tip:
If you change the agent's directory using the `HomeDir` property, remember to copy all of the agents lexicon (vocabulary) files to that directory or the agent will not be able to perform a spell check.

If the `application.properties` file does not exist when the Web Agent is started, Avaya IC creates it as an empty file that can be manually populated. Most entries to populate the `application.properties` file should be provided by Avaya Technical Support. The following are commonly specified options:

- `application.trace.level`. Values:
  - 0 - no logging
  - 4 - critical error logging
  - 5 - exceptions and error logging

- 6 - network message logging
- 7 - step level logging
- 8 - object model event logging
- 9 - constructor level logging
- 10 - UI event logging
- 11 - chat messaging logging
- 12 - email messaging logging
- 15 - full logging

For example: `application.trace.level=10`

- `application.trace.local`. Value true or false. When the value is set to true, the webagent logs are created on the local agent system even if the home directory specified is on the network share. The default location of the webagent logs on the local agent system is: `IC_INSTALL_DIR\IC73\webagent\logs`

  If the value is set to false, the webagent logs are created at the location of the home directory.

  For example:`application.trace.local`=true.

  Note:
  If you do not add `application.trace.local` in the `application.properties` file, then the default behavior is the same as setting `application.trace.local`=true. If you want to write the logs to a shared folder, you must add `application.trace.local`=false in the `application.properties` file.

- `application.trace.mode`. Value 0 or 1. Based on the trace levels for `application.trace.level`, 0 specifies that tracing includes all levels up to and including the value specified. 1 specifies to trace only at the level specified.

  For example: `application.trace.mode=0`

- `application.trace.timestamp`. Value of true or false. When set to true, a new trace file will be created each time the agent logs in and will include the date and time of the file. The naming convention is `webagent_m_d_h_n.log`, where m= month, d = day, h = hour, and n = minute. If set to false, the file name is `webagent.log`.

  For example: `application.trace.timestamp=true`

  Note:
  When setting this value to true, care must be taken to remove old log files as necessary. There is no automatic deletion routine so if this option is set to true for extended periods of time, many log files are created.

- `initial.history.customerinterval.months`. Value: integer value representing the number of months of history that can be retrieved from the History screen of the Web Agent.

  For example: `initial.history.customerinterval.months=2`

- `folder.global.resources.path`. The pathname for the agent's global resources. If blank, the Web Agent uses the path specified in the `HomeDir` property.

  For example: `folder.global.resources.path=c:\Avaya\IC73\agentfiles`

WebACD server configuration options

Configuration parameters that can be set in the `application.properties` file can also be set in the configuration tab of the WebACD server. Parameters set here are used for all tenants and workgroups. When set in this tab, the properties must be preceded with "agentCFG.". For example, `agentCFG.application.trace.level`. For more information about the WACD server, see WebACD server on page 542.

Configuring RONA for the chat channel

The chat channel provides "contact acceptance" return on no answer (RONA) only. This section describes how RONA works in the chat channel, and how to configure the chat channel for RONA.

This section describes how RONA works and includes the following topics:

- About contact acceptance RONA on page 301
- About agent confirmation on page 302
- Configuring agent confirmation for Avaya Agent desktop on page 302
- Configuring agent confirmation for Avaya Agent Web Client on page 302
- About the default timeout on page 303
- Configuring the default timeout for Avaya Agent desktop on page 303
- Configuring the default timeout for Avaya Agent Web Client on page 303
- Changing the default RONA behavior for chat contacts on page 304

About contact acceptance RONA

Contact acceptance RONA occurs only if an agent has the option to accept or reject an incoming chat contact. As soon as the system displays the **Accept contact** dialog box, the timer starts. The timer tracks acceptance of the contact against the default timeout limit set in the Web Agent application properties file.

Contact acceptance RONA requires that you configure Web Agent to require agents to accept the incoming contacts, and that you add a task timeout property to the application.

RONA is activated for an incoming chat contact, if an agent:

- Rejects the chat contact.
- Does not accept or reject the contact within the timeout limit.

In an Automatic blending mode, when only one agent is available and that agent rejects the incoming email or chat contact, by selecting **No** on the contact acceptance dialog box, the system indicates the email or chat channel as busy and closes the dialog box. This shifts the email or chat channel in to the auxiliary mode. However, the agent does not shift to the auxiliary mode.

To enable the email or chat channel, shift the agent in to the auxiliary mode by clicking the agent icon once and click the agent icon again to make the agent available on all the channels.

About agent confirmation

By default, Web Agent automatically accepts all incoming email contacts and chat contacts. Configure agent confirmation in Web Agent on every agent desktop for which you want to enable RONA. RONA cannot work for chat contacts after a chat contact has been accepted.

Important:
After you configure agent confirmation, Web Agent will require agents to confirm acceptance of all incoming email contacts and chat contacts.

Configuring agent confirmation for Avaya Agent desktop

To configure agent confirmation for incoming contacts:

1. In Web Agent, select **Tools** > **Preferences**.
2. In the Web Agent **Preferences** dialog box, select the **Contact** tab.
3. Select the **Wait for agent confirmation before accepting a contact** field.
4. Click **OK**.

Configuring agent confirmation for Avaya Agent Web Client

Use Avaya IC Manager to set the following properties:

- Set the `Agent/Desktop/Chat.AllowDecline` property to **Yes.**
- Set the `Agent/Desktop/Chat.AutoAccept` property to **No**. This will allow the agent to decline the contact when the contact alert is displayed. The default for this property is Yes.
- Set the `Desktop/Chat.PromptOnArrival` property to **Yes** so the agent receives alerts for chat work items.

About the default timeout

After you configure agent confirmation, you need to set the default timeout for the timer. If the agent does not accept or reject the contact within the default timeout, RONA processes the chat contact. The contact can then be rerouted to another qualified agent.

Configuring the default timeout for Avaya Agent desktop

You can configure the default timeout as follows:

- In the Web Agent application properties file on every agent desktop for which you want to enable RONA.
- In a Web Agent application properties file stored in a shared directory. For more information about how to configure Web Agent to access this file in a shared directory, see Customizing the Web Agent on page 299.

Important:
After you configure the default timeout, Web Agent will use this time limit for acceptance of all incoming email contacts and chat contacts.

To configure the default timeout for chat contacts:

1. In a text editor, such as Notepad, open the Web Agent application properties file from the following location:

   `IC_INSTALL_DIR\etc\Webagent\Application.properties`

2. Add the following property to the end of the application properties file:
   `task.autoaccept.time=`*n*

   where n is number of seconds that you want Web Agent to wait for the agent to accept the contact before RONA processes the contact. For example, if you want RONA to handle the contact if an agent does not accept the contact within 30 seconds, add the following property to the file:
   `task.autoaccept.time=30`

3. Save the changes to the application properties file and close the text editor.
4. Restart Web Agent.

Configuring the default timeout for Avaya Agent Web Client

Use Avaya IC Manager to set the `Agent/Desktop/Chat.RONATimeout` property to set the number of seconds that you want the chat work item to alert for the agent before the work is redirected to another agent.

Changing the default RONA behavior for chat contacts

By default, after RONA removes a chat contact from an agent desktop, the WebACD server adds that chat contact to the queue for the agent's workgroup.

You can override the default behavior of the WebACD server after RONA with the ronaenqueueworkgroup_chat configuration parameter for the WebACD server. This parameter has two possible values, as described in the following table:

Value	Description
0	The WebACD server does not add a chat contact to the queue for the agent's workgroup upon RONA.
1	The WebACD server adds a chat contact to the queue for the agent's workgroup upon RONA. This is the default behavior for RONA. You do not need to add this parameter to use this setting.

To use the ronaenqueueworkgroup_chat parameter to change the default RONA behavior:

1. In Avaya IC Manager's **Server** tab, double-click on WebACD server to edit its properties.
2. In the Server Editor dialog box, select the **Configuration** tab.
3. Select **New**.
4. Enter:
   - Name - `ronaenqueueworkgroup_chat`
   - Value - `0`
5. Click **OK**.

Configuring RONA for the email channel

The email channel provides "contact acceptance" and "email activation" return on no answer (RONA). This section describes how RONA works in the email channel, and how to configure the email channel for RONA.

This section includes the following topics:

- Types of RONA for the email channel on page 305
- Configuring contact acceptance RONA for the Avaya Agent desktop on page 305
- Configuring contact acceptance RONA for Avaya Agent Web Client on page 306

- Modifying the time limit for email activation RONA in the Avaya Agent desktop on page 306
- Changing the default RONA behavior for email contacts on page 307

Types of RONA for the email channel

The email channel supports activation RONA, and contact acceptance RONA. This section includes the following topics:

- About email activation RONA on page 305
- About contact acceptance RONA for email on page 305

About email activation RONA

Email activation RONA only works with Avaya Agent desktop. Email activation RONA is enabled by default for the email channel. An agent activates an email contact by opening the contact in Web Agent.

Email activation RONA occurs when an agent accepts an email contact but does not open the contact before the default time limit. The contact can be automatically accepted by Web Agent or manually accepted by the agent. You do not have to configure agent confirmation for Email Activation RONA.

The default time limit is 5 minutes. You can modify this time limit. For more information, see About the default timeout on page 303.

About contact acceptance RONA for email

Contact acceptance RONA works with Avaya Agent desktop and Avaya Agent Web Client. Contact acceptance RONA occurs only if an agent has the option to accept or reject an incoming email contact. As soon as the **Accept contact** dialog box is displayed, a timer starts. The timer tracks acceptance of the contact against the default timeout limit set in the Web Agent application properties file.

RONA is activated for the incoming contact, if the agent:

- Rejects the email contact.
- Does not accept or reject the contact within the timeout limit.

Configuring contact acceptance RONA for the Avaya Agent desktop

To configure contact acceptance RONA, see IC Installation and Configuration.

Configuring contact acceptance RONA for Avaya Agent Web Client

Use Avaya IC Manager to set the following properties:

- Set the `Agent/Desktop/Email.AllowDecline` property to **Yes**
- Set the `Agent/Desktop/Email.AutoAccept` property to **No**. This will allow the agent to decline the contact when the contact alert is displayed. The default for this property is Yes.
- Set the `Desktop/Email.PromptOnArrival` property to **Yes** so the agent receives alerts for email work items.
- Set the `Agent/Desktop/Email.RONATimeout` property to the number of seconds that you want the email work item to alert for an agent before the work is redirected to another agent.

Modifying the time limit for email activation RONA in the Avaya Agent desktop

You change the default time limit for email activation RONA in the Web Agent application properties file. You must modify this file on every agent desktop.

To modify the default time limit for email activation RONA:

1. In a text editor, such as Notepad, open the Web Agent application properties file from the following location:

   `IC_INSTALL_DIR\etc\Webagent\Application.properties`

2. Add the following property to the application properties file: `email.ronatimeout.seconds=`*n*

   where n is number of seconds that you want Web Agent to wait for the agent to open the email contact before RONA processes the contact. For example, if you want RONA to handle the contact if an agent does not open the email contact within 2 minutes, add the following property to the file: `email.ronatimeout.seconds=120`

3. Save the changes to the application properties file and close the text editor.
4. Restart Web Agent.

Changing the default RONA behavior for email contacts

By default, after RONA removes an email contact from an agent desktop, the WebACD server adds that chat contact to the queue for the agent’s workgroup.

You can override the default behavior of the WebACD server after RONA with the ronaenqueueworkgroup_email configuration parameter for the WebACD server. This parameter has two possible values, as described in the following table:

Value	Description
0	The WebACD server does not add an email contact to the queue for the agent's workgroup upon RONA.
1	The WebACD server adds an email contact to the queue for the agent's workgroup upon RONA. This is the default behavior for RONA. You do not need to add this parameter to use this setting.

To use the ronaenqueueworkgroup_email parameter to change the default RONA behavior:

1. In Avaya IC Manager, click the **Server** tab
2. Double-click your WebACD server so that you can edit the properties.
3. In the **Server Editor** dialog box, click the **Configuration** tab.
4. Click **New**.
5. Enter:
   - Name - `ronaenqueueworkgroup_email`
   - Value - `0`
6. Click **OK**.

Creating wrap up, AuxWork, and Logout codes

Using the agent properties in the **Agent/Desktop** section of the **Properties** manager, you can specify whether agents using Avaya Agent desktop or Avaya Agent Web Client are required to select a category, reason, and outcome code when they complete a contact. In addition, you can specify whether agents must select a reason code when they enter AuxWork (set themselves as unavailable without logging out) or log out. For more information about setting these properties, see Agent/Desktop properties on page 577.

To create or edit the codes that are displayed to agents, select **Tools > Codes**.

Avaya IC Manager displays the **Codes Manager**, with the codes associated with each tenant in a tree-view format in the left pane and the details of the selected code in the right pane.

Note:
You must be an administrator in order to create, modify, or delete codes. For more information, see Agent roles on page 227.

Each agent uses a given set of codes, which are grouped into categories (for contact wrap up purposes) and auxiliary groups (for AuxWork and Logout purposes). For details, see Wrap up codes on page 310 and AuxWork and Logout codes on page 313.

General code administration tasks

Whether you are working with wrap up or auxiliary codes, you can set the language for the codes, copy codes, sort codes, or save code changes to the database.

Creating a new code

For information about creating a new code, see one of the following sections:

- Creating wrap up codes
- Creating AuxWork and Logout codes

Setting the language for codes

To set the language for the reason codes:

1. Select **Codes** > **Language**.
2. Select the language you want to use and click **OK**.

Note:
The language setting applies to all reason codes. If you want to work in multiple languages, create the code in one language and enter the **Agent Displayed Value** for that language. Then change the **Language** setting and enter a new **Display Name** for the codes you have already created.

Copying codes

When you copy codes in the **Codes Manager**, Avaya IC Manager does not create a true copy. Instead, it creates a link between the original code and the copy. If you edit or delete either the original code or the copy, Avaya IC Manager changes or deletes the code everywhere that it displays.

If you want to copy a code:

1. Select the node you want to copy and select **Codes** > **Copy**.
2. Select the code under which you want the copy to appear and select **Codes** > **Paste**.

Sorting codes

If you want to sort codes automatically, select **Codes** > **Auto Sort**.

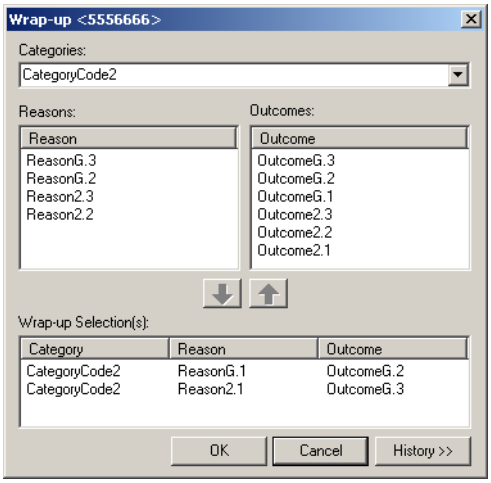
Saving code changes

If you want to have your changes automatically saved to the database, select **Codes > Auto Commit**. Otherwise, you need to select **Save** on the toolbar to save your changes.

Wrap up codes

If the **Agent/Desktop/WrapUpEnabled** property is set to **Yes** for an agent, then whenever that agent completes a contact, Avaya Agent displays the Wrap Up dialog box. (For details about setting the wrap up property, see Agent/Desktop properties on page 577.)

The following illustration shows a sample wrap up dialog:



This dialog requires the agent to select three Wrap Up codes:

Category code: The purpose of a customer's initial reason for contacting that agent, or the intent of the work performed (for example, Auto Loan, Boat Loan, Home Loan).

Reason code: The reason associated with the contact (for example, 3 year loan application, 5 year loan application, request account balance). When the agent selects a category code, Avaya Agent limits the list of possible reason codes to those that have been associated with the selected category code plus any generic reason codes that you have defined.

Outcome code: The result of the contact with the customer (for example, application submitted, account balance provided). When the agent selects a category code, Avaya Agent limits the list of possible outcome codes to those that have been associated with the selected category code plus any generic outcome codes that you have defined.

For example, if you have defined the following codes:

Category Group	Reason Codes	Outcome Codes
Auto Loans	3 year loan application 5 year loan application car insurance	application submitted insurance options discussed
Boat Loans	3 year loan application boat insurance	application submitted insurance options discussed
Home Loans	15 year loan application 30 year loan application home insurance	application submitted insurance options discussed
Generic Codes	account balance request	account balance provided

When an agent selects the Auto Loan category, they are presented with the reason codes from the Auto Loans and Generic categories:

- 3 year loan application
- 5 year loan application
- car insurance
- account balance request.

In addition, they are shown the following outcome codes:

- application submitted
- insurance options discussed
- account balance provided.

When you create wrap up codes, remember that agents will need to select a code from the list as quickly as possible. Make sure that your codes cover all possible categories, reasons, and outcomes without overlapping. The descriptions you assign should be short but clear.

Creating wrap up codes

To create a new wrap up code:

1. In the Avaya IC Manager, select **Tools** > **Codes**.

   The Codes Manager window opens.
2. In the left pane of Codes Manager, expand the tenant for whom you want to create a new code. The associated category groups are displayed.
3. Expand **Category Groups**. Refer To create a new category group on page 312.
4. Expand a Category code. Right-click Wrapup codes, select **New** to create a wrapup code.

5. Enter the following details:
   - **Name**: The name of the code. This name must be unique and different from the AuxGroup name.
   - **Displayed Name**: The localized text string that Avaya Agent displays when an agent requests a list of wrap up codes. Ensure that the string is short but descriptive.
   - **Description**: The complete description of the code.
6. Click **OK**.

To create an outcome code:

1. In **Codes Manager**, expand a tenant.
2. Expand **Category Groups**.
3. In a particular category, expand **Wrapup Codes** and navigate to a Wrapup Code.
4. Right click **Outcome Codes** and select **New**.

To create a reason code

1. In **Codes Manager**, expand a tenant.
2. Expand **Category Groups**.
3. In a particular category, expand **Wrapup Codes** and navigate to a Wrapup Code.
4. Right click **Reason Codes** and select **New**.

To create a generic code

1. In **Codes Manager**, expand a tenant.
2. Expand **Category Groups**.
3. In a category group, expand **Wrapup Codes**.
4. Right-click **Generic Codes** and select **New**.

Note:
The outcome and reason codes need to be populated for at least one Wrapup codes, for the wrap up to appear at the agent end. The generic code is always displayed to the agent, under all Wrapup codes.

To create a new category group

1. In the **Code Manager**, expand a tenant.
2. Right-click **Category Groups**.
3. Click **New**.

Associating wrap up codes with agents

Once you have created codes and grouped them by tenant and category, you need to denote which agents will use which code groups. To do so, set the **DefaultCategoryGroup** and **DefaultTenant** properties in the **Agent/Desktop/WrapUpDialog** subsection. You can also use the **Required** property in this subsection to force agents to enter a wrap up code after every contact. (For more information, see Agent/Desktop/WrapUpDialog properties on page 630.)

AuxWork and Logout codes

If you want agents to specify a reason why they are making themselves unavailable (going into AuxWork mode) or logging out, you can set up AuxWork and Logout codes. If you enable this functionality, agents will be asked to select a code from the specified list before their status is changed to unavailable.

Once you create the AuxWork and Logout codes, you organize them into Auxiliary Groups, and then associate those Auxiliary Groups with different agents. By default, Avaya IC includes an Auxiliary Group called **SystemAuxGroup**. This group defines two default values:

Code	Description
0	Used for AuxWork on Login. If the Avaya IC system automatically puts the agent into AuxWork mode as soon as he or she logs in, it uses this reason code to explain.
1	Used for No Available Reason. If the agent does not select an AuxWork or Logout code, then the system uses this code to denote that.

When you create your codes, make sure that you do *not* use either 0 or 1. If you do, you will need to change the values of the system codes so that each code has a unique value. For details, see Changing the default system AuxWork codes on page 315.

Creating auxiliary groups

To create an auxiliary group:

1. Select **Tools** > **Codes**.
2. Expand the **IC** system entity in the left-hand pane, and navigate to the tenant you want to add the group to.
3. Under that tenant, select **Auxiliary Groups**.
4. Select **Codes > New**. Avaya IC displays the **Aux Group Editor**.
5. Enter the name, display name, and description of the Auxiliary Group that you want to create. The name must be unique and different from the name of the Wrapup category group name

6. Click **OK**.

Repeat this procedure for all of the Auxiliary Groups you want to create for this tenant.

Creating AuxWork and Logout codes

To create an AuxWork or Logout code:

1. Select **Tools** > **Codes**.
2. Expand the **IC** system entity in the left-hand pane, and navigate to the tenant you want to add the code to.
3. Expand **SystemAuxGroup** in the left-hand pane and select either **Busy Codes** or **Logout Codes**.
4. Select **Codes** > **New**. Avaya IC displays the **Reason Editor** for the type of code you selected.
5. Select a **Name** from the drop-down list. Remember that 0 and 1 are used by the default system variables. If you select either of these names, you will need to change the system variables accordingly. (For details, see AuxWork and Logout codes on page 313.)

   Note:
   AuxWork and Logout code names can be between 0 and 99. If you are using a Avaya Communication Manager switch, these codes are written to the switch as well as the ADU.

6. Enter the name that Avaya Agent will display to the agent.
7. Enter a description of the code.
8. Click **OK**.

Repeat this procedure for each code you want to add.

Associating agents and auxiliary groups

Once you have created your Auxiliary Groups, you can use the **Agent/Desktop** properties to associate them with agents. You need to set the following properties (for more information, see Agent/Desktop properties on page 577):

Property	Description
AuxGroup	The name of the Auxiliary Group you defined in the Codes table.
AuxGroupTenant	The tenant that this Auxiliary Group is associated with.
AuxReasonCodesEnabled	If you want agents to specify an AuxWork code, set this property to Yes. Otherwise, set it to No.
LogoutReasonCodesEnabled	If you want agents to specify a Logout code, set this property to Yes. Otherwise, set it to No.

Once you have set these properties for an agent, they will see the AuxWork and Logout codes defined by the Auxiliary Group named in **AuxGroup**.

Changing the default system AuxWork codes

The default **Agent/Desktop** settings for the system AuxWork properties are:

- SystemAuxGroup = SystemAuxGroup
- SystemAuxGroupTenant = DefaultTenant
- AuxLoginReasonCode = 0
- AuxNotAvailableReasonCode = 1

To change the default system AuxWork names:

1. Select **Tools** > **Codes**.
2. In the left-hand pane, expand the **Auxiliary Groups** under the **DefaultTenant**.
3. Expand the **SystemAuxGroup**.
4. To change the default **AuxLoginReasonCode**:
   a. In the left-hand pane, select **Busy Codes**.
   b. In the right-hand pane, double-click the **AuxNotAvailableReasonCode** entry.
   c. Change the name to the desired value. Make sure that this value is unique.
5. To change the default **AuxNotAvailableReasonCode**:
   a. In the left-hand pane, select **Logout Codes**.
   b. In the right-hand pane, double-click the **AuxNotAvailableReasonCode** entry.
   c. Change the name to the desired value. Make sure that this value is unique.
6. Change the **Agent/Desktop** settings listed above to match the new values. For details about changing agent property values, see Changing property values on page 373.

Audio and visual notifications for the chat channel

Avaya IC 7.3.5 enhances chat notifications:

- Audio notifications
- Web Agent icon flashing
- Color coding of chat lists

For more information about the audio and visual notification enhancements, see *Avaya Interaction Center and Avaya Operational Analyst Overview and Specification*.

Configuring audio and visual notifications for the chat channel

1. To play an alert when a contact arrives, do the following steps on the Avaya Agent Rich Client (AARC) machine:
   a. In Web Agent, select **Tools** > **Preferences**.
   b. In the Web Agent **Preferences** dialog box, select the **Contact** tab.
   c. Click **Alert with sound when a new contact Arrives**.
   d. Click **OK**.
2. On the AARC machine, add the following properties to the `Application.properties` file at `AVAYA_IC_73_HOME\Webagent` for audio notifications:
   - `webagent.sounds.enabled=true`
   - `sounds.oncustomeralert.enabled=true`
   - `mediaspecific.sounds.onarrival = true`

   To customize the sound alerts to indicate that customers sent a chat response, see Customizing sound alerts on page 317.
3. In the `AgentPreferences.xml` file, customize the `Alarming` property to indicate the number of times and the intervals at which the Web Agent icon flashes after a customer responds to a chat message.

   The default value of the number of times that the Web Agent icon flashes is three and the default rate at which the icon flashes is 800 milliseconds. The default `Alarming` property is as follows: `<Alarming flashes_number="3" interval="800" />`.
4. Add the following properties on the Avaya IC Manager machine for color coding of chat lists:
   a. In IC Manager, on the main menu, select **Tools > Property Declarations**.

      Avaya IC Manager displays the **Property Declarations** dialog box.
   b. In **Property Section**, click **Agent/Desktop/Chat/Application** and add the following properties:
      - `SLATimings` with `string` set as the datatype
      - `ChatListBGandTextColors` with `string` set as the datatype
      - `EnableChatListColorCoding` with `boolean` set as the datatype
   c. Click **OK**.
   d. In IC Manager, on the main menu, select **Tools > Groups**.

      Avaya IC Manager displays the **Group Manager** dialog box.
   e. Click the **Properties** tab.
   f. For configuring color coding in chat list, do the following:

1. In **Sections**, click **Agent/Desktop/Chat/Application**, add `SLATimings`, and set the Service Level Agreement (SLA) timing for agent response to chat messages. You can set up to three SLA levels. Based on the SLA levels, AARC changes the background color for chat lists.

   You must specify the SLA time values in seconds, and the values must be distinct and in increasing order. If you enter wrong values for `SLATimings`, the default values of 20, 40, and 60 are used.

   For example, you can add `SLATimings` with values set as 20, 30, 40. The value of 20, 30, 40 corresponds to SLA1, SLA2, and SLA3. SLA3 is the highest wait time for agents to respond to chat messages.

2. To color code the chat lists, in **Sections**, click **Agent/Desktop/Chat/Application**, add `EnableChatListColorCoding`, and set the value to `Yes`.

   If you set `EnableChatListColorCoding` to `No` AARC does not display colors in the chat list based on the SLA levels set for agents to respond to chat messages.

3. In **Sections**, click **Agent/Desktop/Chat/Application**, add `ChatListBGandTextColors`, and set the background and text color that corresponds to the SLA time values set.

   You must use hexa-equivalents of RGB values for the color coding. The default values for `ChatListBGandTextColors` is E4DFEC,E6B9B8,D99694,C0504D,000000,000000,000000,FFFF00. The first four hexa values correspond to the background colors, the last four colors correspond to the text color. The hexa-equivalents of RGB are case insensitive and must not be preceded by '0x'. If you enter wrong values for `ChatListBGandTextColors`, the default values are used.

Customizing sound alerts

1. For customizing the sound alerts to indicate that customers have sent a chat response, in the `AVAYA_IC_73_HOME\Webagent` folder, create a `ClientInterface_en.properties` file on each agent machine and add the following properites:

   ```
   task.livehelp.arrived=unlock.wav
   livehelp.customer.action=unlock.wav
   ```

2. For customizing the sound alerts for an incoming chat contact add the following property to the `ClientInterface_en.properties` file:

   ```
   task.livehelp.arrived =<Path of the sound file relative to
   AVAYA_IC73_HOME\Webagent folder>/<Name of sound file>.wav
   ```

Customizing the window for the popped out chat tab

Agents can pop out a tab with a chat task as a separate window. The separate window is independent and has its own toolbar. Agents can also pop-in the separate window back as a chat task on the main window.

You can customize the dimensions and the close operations for the popped out window.

1. In the `AgentPreferences.xml` file, customize the `SeparateChatWindow` property.

   By default, the `SeparateChatWindow` property is present as follows:

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

   For the close operation you must specify one the following values:

   - 1 - do nothing
   - 2 - pop-in
   - 3 - close window, but keep in the window in the task list. This option does not affect the session.

   If you specify an incorrect value to the `closeOperation` attribute, the default value of 1 is used.

   You must specify the `height` and `width` attributes in pixels. If you do not specify any value or specify incorrect value, the following default values are used:

   - `Width`: The preferred size for transcript panel, which is usually the width of the taskbar.
   - `Height`: Half the height of the screen dimensions.

Chapter 13: Document search facilities

Avaya Interaction Center (Avaya IC) allows you to create document collections that your agents can search for information. The Web Self-Service component within Web Management consists of an online database of question and answer pairs grouped by topic. Agents and customers can search this database using the component's HTML interface.

If you want to let customers search through your database, or if you want your agents to have web access to your database, then you need to use the Web Self-Service component.

This section contains the following topics:

- Setting up the Web Self-Service feature on page 320
- Administering the FAQ database on page 321

Setting up the Web Self-Service feature

The Web Management component in Avaya IC includes a Web Self-Service feature that lets employees or customers search for answers to common problems on their own. The feature includes the FAQ (Frequently Asked Questions) database along with HTML pages that allows you search the database, submit new items, and administer the current items.

The FAQ database is arranged as a series of question and answer pairs. Each pair is called a document, and the documents are grouped together under topics. This gives rise to a tree-like hierarchy, in which the topics are called branches and the documents are called leaves.

You can define a FAQ database for each tenant (organization) in the Avaya IC system. You can also define a FAQ database for each language that you have enabled for a particular tenant. (For details, see Tenants on page 241 and Enabling website language options on page 327.)

In order to use the Web Self-Service Feature:

1. Set up a search engine to search the pages. If you want to use Avaya FTSE, see IC Installation and Configuration.
2. Create the FAQ database. For details, see Administering the FAQ database on page 321.

Administering the FAQ database

You can view, search, edit, and add to the documents in the FAQ database using the Supervisor Control menu. To access this menu:

1. In Avaya IC Manager, select **Services > Web Response Unit**.

   Avaya IC Manager opens the IC Website Administration Tool in an HTML browser window displaying the **Welcome to the Interaction Center Website Self-Service** page.

2. Select **Web Self-Service Console** in the menu on the left-hand side of the page.

Note:
The following sections on administering the FAQ database assume that you are starting from this location.

This section includes the following topics:

- Managing the FAQ database on page 321
- Submitting new documents on page 322
- Reviewing agent-proposed documents on page 323
- Editing and deleting existing documents on page 324
- Searching for specific documents on page 324

Managing the FAQ database

To view or edit documents in the FAQ database:

1. Select **Manage FAQ** in the left-hand pane.
2. Select the tenant whose FAQ database you want to work with from the drop-down list and then select **Manage FAQ**.

   The IC Website Administration Tool displays the FAQ database for the selected tenant, showing the document titles and the organizational relationship between them.

3. If you want to view the FAQ documents that are in different language, select that language from the drop-down list at the top of the page.

Note:
You might not be able to search on FAQ documents that are 3K or larger with Oracle or DB2 databases. Try to limit FAQ documents to less than 3K in size.

Submitting new documents

To submit a new document:

1. Select **Manage FAQ** in the **Web Self-Service** menu, select the tenant, and then select **Manage FAQ**.
2. Select the topic or document under which you want to add the new document. If you select an existing document, Web Management automatically promotes the existing document into a topic (or branch node) and adds the new document (or leaf node) under it.

   Note:
   You cannot have more than 2,500 documents assigned to a single topic. For better performance the document tree must not have numerous subtopics, or have more than 500 documents assigned to a single topic.
3. Click **Submit**. Web Management displays the **Submit a Document** page.
4. Enter the name of the document in the **Title** field (ASCII characters only). If you have enabled multiple languages for your website, then this is the title that will always display in the administrative view for the Web Self-Service database. The language-specific title below is the one that will be displayed to end users based on their language settings.
5. In the **Language Specific Document Parts** section, you can specify:
   - **Title**. Web Management displays this title to the user. You may want all of the titles of your documents to be in the form of a question.
   - The source for the document:
     - If the document is an external URL, select **Internet Link** and enter the complete address, including the protocol (for example `HTTP://`), in the associated text field.
     - If the document is text, select **Text** and enter the document's text in the associated field. This text must be entered in ASCII format; you cannot use any HTML coding.
6. In the **Routing Attributes** section, you can specify:
   - **Tasktype**. Select the task type from the **Tasktype** drop-down list.

   Note:
   Tasktypes are not used in Avaya IC. This field is provided for backward compatibility with earlier versions of Avaya IC.
   - **Mail Account**. If there is an email account associated with this document, select it from the drop-down list. If the user elects to send mail from the website, Web Management uses the email account associated with the most recently viewed Web Self-Service document to determine where that email should be sent.
   - **Routing Hints**. You can select up to two routing hints in the **Routing Hint** drop-down lists.

   Note:
   The **Routing Attributes** are visible only to the Supervisors and Administrators.

Note:
Only one routing hint is supported in the out-of-the-box configuration of Avaya IC. For more information about adding routing hints to the Configuration tab in Avaya IC Manager, see WorkFlow table folder on page 150. For information about implementing Routing Hints, see *Avaya IC Media Workflow Reference*.

7. Click **Submit**. Web Management displays a page informing you that the document was successfully posted. Click **Continue** to return to the FAQ database page.

If you are authorized to add documents directly to the FAQ database, Web Management adds your document immediately. Otherwise, Web Management places your document in a queue where it can be reviewed by an administrator or supervisor. Once the document is accepted, Web Management adds it to the FAQ database. For more information, see Reviewing agent-proposed documents on page 323.

Reviewing agent-proposed documents

When an agent submits a new document, Web Management places it in the Proposed Document queue. An administrator or supervisor needs to review each proposed document and either accept or reject it.

To view proposed documents:

1. Select **Manage Proposed FAQ** to open the **Manage Proposed FAQ** page.
2. Select the tenant and language whose proposed documents you want to view from the drop-down lists.
3. Select **Manage Proposed FAQ** to view the list of proposed documents on the **Approve Document** page.
4. Select a proposed document and read it.
5. Click **Approve** to approve the proposed document or **Reject** to reject it. If you approve a proposed document, Web Management adds it to the database. If you reject it, Web Management deletes it from queue and does not delete it from the database.

Note:
If you are a supervisor, you can update the **Routing Attributes** for a document only after you approve it. For updating the **Routing Attributes**, see Editing and deleting existing documents on page 324.

Editing and deleting existing documents

Once you have selected a document, you can view, edit, or delete it.

To select a document:

1. Select **Manage FAQ** in the **Web Self-Service** menu, select the tenant, and then select **Manage FAQ**.
2. Navigate to the document you want to view and select it in the list of documents.

   Web Management displays the selected document beneath the line separating the list of documents from the text of the selected document.

To edit the currently-selected document:

1. Click **Update** to open the **Submit a Document** page.
2. Change the text as desired.
3. When you are finished, Click **Update**.

Deleting documents

You cannot delete the root (or first) document in the FAQ. To delete any other document, select that document and select Delete. Web Management removes the document from the FAQ database.

If you delete a topic that has other FAQ elements (documents or topics) below it, Web Management does *not* delete those elements. Instead, it moves them up one level and attaches them to the parent of the deleted topic.

Searching for specific documents

To search for a specific document:

1. Select **Search FAQ**.
2. Select a tenant from the drop-down list and select **Search FAQ**.
3. Enter any characters or words you want to find in the FAQ database and select **Go**.

   Web Management displays a list of results beneath the line of the **Search FAQ** page.
4. Select the name of any document in the list of results to access that document.

Chapter 14: Tenant websites

You can customize a website for each tenant in the environment so it has its own look and feel, and each website can appear in multiple languages. For details, see Tenants on page 241.

For example, if you host two tenants, one a computer repair shop and the other a toy seller, you could store both websites on the same server, customize them with the same application, and yet have two completely different websites from a customer's point of view.

Note:
Some of the MultiTenant features are not fully integrated with all of the Avaya IC servers. For assistance in creating a multitenant environment, contact Avaya CRM professional services.

After creating a tenant's website, you can also create customer accounts so that you can control who can log into the site. The administrator determines what information is required when an agent or user requests a login account, and whether customers can create their own accounts on the fly.

The Web Management component of Avaya Interaction Center (Avaya IC) includes a set of HTML pages, collectively known as the IC Website Administration Tool, that allows you:

- Enable multiple languages for your tenant websites
- Customize tenant websites
- Customize the account information Web Management collects when an agent or customer creates an account
- Manage customer accounts
- Monitor WebACD server status (for more information, see WebACD server statistics on page 83)
- Manage your Web Self-Service (FAQ) database.

This section contains the following topics:

- Enabling website language options on page 327
- Customizing tenant websites on page 329
- Customizing account information on page 332
- Working with customer accounts on page 334
- Setting up Shared Browsing on page 340
- Using the DataWake feature on page 341
- Setting up DataWake filters on page 346
- Viewing DataWake records on page 350
- Using the Email History feature on page 351

- Using the Chat History feature on page 357

Enabling website language options

You can enable multiple languages for use within a tenant's website. When you do so, you select one of the languages to be the default, and all of the tenant properties automatically inherit the settings for properties in the default language. You can override this inheritance for any property you want to vary within each language. (For details, see Customizing tenant website properties on page 330.)

This capability lets you quickly create multi-lingual versions of a website, all of which work and act in an identical manner. It also allows you change properties for the default language and have those changes automatically propagate to the other languages unless you have specifically overridden that inheritance.

This section contains the following topics:

- Adding a new language on page 327
- Enabling a language for a tenant on page 328
- Deleting a language on page 328
- Internationalized language options on page 328

Adding a new language

To a add new language:

1. In Avaya IC Manager, select **Services** > **MultiTenancy Administration**.

   Avaya IC Manager opens the web-based IC Website Administration Tool and displays the **Welcome to the Interaction Center Website Multi-Tenant Administration** page.

2. Select **Define Languages** in the **Tenants Admin** menu.
3. Enter the language code, country code, default description, and default display text in the **Properties** box.

   Important:
   If you are going to import the international website properties that Avaya IC provides out-of-the-box, you should *not* enter a country code. For more information, see Internationalized language options on page 328.

4. When you are done, select **Add Language**.

   The IC Website Administration Tool redisplays the **Enable Languages** page with the new language listed in the language box, and Web Management automatically enables this language for the Default tenant.

Enabling a language for a tenant

To enable a language for a tenant:

1. Select **Enable Languages** in the **Tenants Admin** menu. The IC Website Administration Tool displays the **Enable Languages** page.
2. Select the desired tenant and select **Customize Tenant Languages**.
3. For this tenant, you can:
   - Enter new display text for the language.
   - Allow the tenant to use this language by selecting the **Enabled** check box.
   - Set this as the tenant's default language by selecting **Default**.
4. Click **Edit Languages** to submit your changes.

Note:
You cannot change the Default Language (English) for the Default Tenant.

Deleting a language

To delete a language:

1. Select **Define Languages** in the **Tenants Admin** menu.
2. Select the **Delete** check box for each language that you want to delete.
3. Click **Delete**.

Tip:
If you want to disable a language without deleting it, clear the **Enabled** check box for that language on the **Enable Languages** page.

Internationalized language options

The International version of Avaya IC contains localized website properties that can be used to add language-specific web page and chat applet text to your installation. These localized properties use the standard Avaya IC language codes to identify which country they are associated with, but they do *not* use the country code discussed in Enabling website language options on page 327.

In order to use the out-of-the-box localized properties:

1. If you have not already done so, import the localized properties as described in IC Installation and Configuration.
2. Enable the languages you want to use on the website, making sure you use the standard Avaya IC language codes and you do *not* enter a country code.
3. Restart the website server so that it recognizes the new language codes and, if necessary, uploads the localized seed data from the database.

If you want the tenant's website to recognize several variations on a language, you can create new language codes comprised of one of the standard two-letter code combined with a custom two letter Country Code. (For example, to create a Castilian variation of Spanish, you could define a language with the language code `es` and the country code `CA`. Web Management stores that language code as `es-CA`.)

Important:
While you can use this language code variation on the website, it will not be recognized in any other part of the Avaya IC system. So, for example, you cannot use the es-CA code to specify the language for an AuxWork or Logout code.

Any language whose code begins with one of the standard two-letter abbreviations, defaults to the internationalized property settings for that language. That means you only need to change the values for those properties that differ between the language variation and the root language.

Note:
Any language whose first two letters do not match, one of the standard codes default to the English (`en`) property values.

Customizing tenant websites

You can customize tenant websites by:

- Changing the settings for basic properties using the IC Website Administration Tool. These properties can be changed on the fly by anyone with administration privileges. For details, see Customizing tenant website properties on page 330.
- Replicating the underlying source code and making changes to that code. Changing the code needs to be done very carefully by an experienced website designer, but it gives you the maximum flexibility when it comes to customizing your tenant websites. For details, see Customizing tenant source code on page 331.
- Specifying the location of the tenant's index page. For details, see Specifying the URL for the tenant's index page on page 332.

Note:
If a customer sends an email from the website, the email address that Web Management uses is the one associated with the last FAQ document that the customer viewed. For details, see Managing the FAQ database on page 321.

Customizing tenant website properties

The IC Website Administration Tool allows you modify all of the tenant's website properties. To do so:

1. In Avaya IC Manager, select **Services** > **MultiTenancy Administration**.

   Avaya IC Manager opens the web-based IC Website Administration Tool and displays the **Welcome to the Interaction Center Website Multi-Tenant Administration** page.
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, and then select **Customize Tenant**. The IC Website Administration Tool displays the **Customize Tenant** page.
4. Select the language properties you want to set from the **Select Language** drop-down list at the top of the page.
5. From this page you can view and modify all tenant properties in a table organized by group.
   - To view all properties, select **All Properties**. The IC Website Administration Tool displays all of the tenant's properties, sorted alphabetically. The prefix of each property describes the group which the property belongs to. (For example, all chat properties start with "`chat.`")
   - To view only those properties associated with a specific group, select the group name from the list.
6. If you want to override the inherited value for a given property, clear the check box in the (*) column for that property. You can then enter a new value for that property.
7. When you are finished modifying the properties you wish to change, select **Update Data** at the bottom of the page.

Additional property information

Generally, the Description and Suggested Values column provides enough information for you to fill in a particular field. However, there are a few things that you need to keep in mind:

- There is no error checking on these fields. If you enter a value that does not fall within the range of expected values (as defined in the Suggested Value column), it may appear to be accepted by the system even though it will not work.
- If a field takes a 0 or 1, then 0 always means "false", "no", "disabled" or "closed" while 1 means "true", "yes", "enabled", or "open".
- If you enter a URL for any page that is not stored in the Web Management system, it could cause parsing problems and the page may be displayed incorrectly.

- You can indicate different fonts for different browsers by separating the font names with commas. For example, if Internet Explorer supports Arial while Netscape supports Helvetica, you could enter `Arial, Helvetica` in the field.

Customizing tenant source code

Web Management uses a servlet engine to display the JSP files that make up each tenant's website. The servlet engine loads the pages from a single *context* (website application). A context is represented by a root directory on the server, while all tenants within that context have their own subdirectory under that root. By default, all tenants use the same source code, and customizations are done using the tenant properties described in Customizing tenant website properties on page 330.

If you want to extensively customize a particular tenant, you can maintain a separate copy of the source code files in a different directory. To do so:

1. Create a new subdirectory under the existing context directory (for example, under `website`).
2. Copy all files from `IC_INSTALL_DIR\etc\comp\website\public` into the newly-created tenant subdirectory.
3. Make desired changes to the images, JSP files, XSL stylesheets, or other source files.

For example, if your default tenant is stored in `IC_INSTALL_DIR\etc\comp\website\public`, then the context directory is `IC_INSTALL_DIR\etc\comp\website`. Any customer accessing this default tenant would use the URL `http://www.host.com/website/public`.

To add a tenant called "sales", you would create a subdirectory called `c:\avaya\ic73\comp\website\sales` and copy the files from `IC_INSTALL_DIR\etc\comp\website\public` into that subdirectory. Customers would use the URL `http://www.host.com/website/sales` to access the new tenant.

After you do the copy, the Sales tenant has all the same property settings as the DefaultTenant. You can modify the source code, or you can work with the Tenant Properties described in Customizing tenant website properties on page 330. At the very least, you need to change the source directory metadata property, `website.pages.public`.

Specifying the URL for the tenant's index page

If customers do not specify a specific tenant's index page when they access the website, Web Management displays a generic page allowing them to select the tenant they want to visit. This solution is useful if customers only remember part of your website's URL, but for any direct links that you publish via web, email, or in print, you should specify the complete path.

The format of a tenant's index page URL depends on how you customized the website:

- If you created the new tenants in Avaya IC Manager and customized just the Tenant Properties (as described in Customizing tenant website properties on page 330), then you can access the index page by specifying the tenant name and language in the standard URL. For example, if you have a tenant called `sales`, the index page URL would be:

```
http://www.avaya.com/website/public/index.jsp?aicTenant=sales&aicLanguage=en
```

Note:
You can omit the language parameter if there is only one language enabled for the website.

- If you changed the source code (as described in Customizing tenant source code on page 331), then you can access the index page by entering the tenant subdirectory name in place of `public` in the above URL.

  For example, if there is only one tenant, with only one enabled language, using this source code directory, you would specify:

  ```
  http://www.host.com/website/sales
  ```

  Otherwise, you would specify:

```
http://www.host.com/website/sales/index.jsp?aicTenant=sales&aicLanguage=en
```

Customizing account information

The User Properties feature allows you customize the data that appears in the Create Customer Account page that is displayed to both customers and administrators. You can change standard form elements such as labels, whether text entered into a field is obscured, or whether a field displays at all. In addition, you can add new properties to the form in case your company wants to collect additional information.

For more information, see:

- Customizing standard properties on page 333
- Adding new user properties on page 333

Customizing standard properties

To customize standard user properties information:

1. In Avaya IC Manager, select **Services** > **MultiTenancy Administration** to open the **Welcome to MultiTenant Administration** page.
2. Select **User Properties** under **Tenants Admin**.
3. Select the tenant whose user properties you want to modify from the drop-down list, and select **User Properties**.
4. Each field on the User Properties page has the following properties:
   - **Attributes**: The name of the metadata key for the property. This field is not editable.
   - **Caption**: The associated caption that is displayed in the form. The language-specific captions for user properties can be set by changing the metadata properties beginning with `account.text.userprop`. For details, see Customizing tenant website properties on page 330.
   - **Obscure**: Determines whether or not the value entered by the user is displayed. This is usually set to **True** for password fields and **False** for other fields.
   - **Weight**: Determines the priority of the property, with a lower value indicating a higher priority. The weight determines the order in which the fields are displayed on the Create Customer Account form: the field with the lowest weight is displayed first, then the field with the next lowest weight, and so on. (If two or more fields have the same weight, they appear in alphabetical order.) Valid values range from 0 to 100.
   - **Protect:** Once an account is created, if this field is set to True, the user will not be able to change the contents of the field when modifying their account information. When creating a new account, the user will always be able to enter the contents of any required fields.
   - **Visible**: Determines whether or not the field will be visible to the user.
5. Set the user options as desired. When you're done, select **Update**.

Adding new user properties

You can add as many new free-form text properties as you want. To do so:

1. Open the **User Properties** page and scroll to the **Extended Properties** section near the bottom of the page.
2. Select **Add New Property** to open the **Add Extended User Property** page.
3. Enter a property name and caption, then select **Update**.
4. You can now set the other property values as described in Customizing standard properties on page 333.

Tip:
By default, the customer's title is chosen from a drop-down list. If you want the customer to be able to enter any title, hide the `userprop.opt.title` property and add a new extended property for the customer's title.

Editing or deleting extended user properties

To edit the attributes for an extended property, go to the **Extended Properties** section, make your desired changes and select **Update Properties**.

To change the name of the property, click on that name, make your changes, and then select Update.

To delete an extended property:

1. In the **Extended Properties** section, click on the name of the property you want to delete.
2. Click **Delete**.
3. Confirm the deletion at the prompt.

Working with customer accounts

You can either allow customers create their own accounts on the fly, or you can create an account for each customer and tell them their user name and password. The user names must be alphanumeric. The first character of the user name must be a letter, not a number.

Note:
Whether customers can create their own accounts is controlled by the `security.usercreation` property. For details on setting it, see Changing properties on page 372.

By default, each customer using Web Management *must* have a separate account, two customers *cannot* log in at the same time under the same login ID.

The way Web Management manages customer accounts is controlled by out-of-the-box workflows created with the Workflow Designer. If the default process does not fit your business model, then you can change the flows to fit your needs. For details about the default flows, see Understanding the default account management process on page 337. For details about modifying flows or using the Workflow Designer, see *Avaya Workflow Designer User Guide*.

This section contains the following topics:

- Creating customer accounts on page 335
- Modifying customer accounts on page 335
- Enabling and disabling customer accounts on page 336
- Understanding the default account management process on page 337

Creating customer accounts

To create customer accounts:

1. In Avaya IC Manager, select **Services** > **MultiTenancy Administration** to open the **Welcome to MultiTenant Administration** page.
2. Select **Create Customer Account** under **Customer Management**.
3. Select the tenant to associate with this customer from the **Select a Tenant** drop-down list.
4. Select **Create Customer** to open the **Create Customer Account** page.
5. Enter the appropriate information in the fields. A pencil following each field indicates that it is required.

   Tip:
   The user name must be at least three characters long and the email address should be in the format `name@somewhere.com`.

6. Select **Create** to add the account to the database.

Modifying customer accounts

Use the Manage Customer Accounts feature to view information about a customer or to modify a customer account.

To modify customer accounts:

1. In Avaya IC Manager, select **Services** > **MultiTenancy Administration** to open the **Welcome to MultiTenant Administration** page.
2. Select **Manage Customer Accounts** under **Customer Management**.
3. Enter the customer's user name in the **Name** field, *without* the "@tenantname" portion of the user name. You can also enter an asterisk (*) to view all customers, or use it as a wildcard following a partial user name in the Name field. (For example, br* will match Brian, Bryan, Bryce, etc.)

   Tip:
   If you enter a customer's full name and search does not find that customer, add an asterisk to the end of the customer's user name and repeat the search.

4. Select **Find** to open the **Customer Account Management** page displaying any customers from any tenant that match the search string.
5. Select the customer name from the list, then select **Modify** to view the customer's account information.
6. Enter the appropriate information in the fields that you want to change.

7. Select **Edit**.

Enabling and disabling customer accounts

When you disable a current customer account, Web Management keeps the information in the database in case you want to re-enable it later. To actually delete a customer account from the database, you need to use your database administration tool.

Note:

Before you disable an account, ensure that the customer is not currently taking part in a chat session and that they don't have an email pending in the system. To do so, check the list of currently running tasks for the customer's name and email address. For more information, see Working with WebACD tasks on page 84.

To enable or disable an existing customer account:

1. In Avaya IC Manager, select **Services** > **MultiTenancy Administration** to open the **Welcome to MultiTenant Administration** page.
2. Select **Manage Customer Accounts** under **Customer Management**.
3. Enter the customer's user name in the **Name** field. You can also enter an asterisk (*) to view all customers, or use it as a wildcard following a partial tenant name in the Name field. (For example, br* will match Brian, Bryan, Bryce, etc.)
4. Select the customer name from the list and select **Disable** or **Enable**. Confirm the action when prompted.

Understanding the default account management process

Web Management manages customer account records using out-of-the-box workflows created with Workflow Designer. The default workflows are:

- AddCustomer (addcustomer.qfd): Adds a new customer record to the database. This flow requires customer information, tenant ID, and an unique email address for the customer. (For details, see AddCustomer on page 337.)
- UpdateCustomer (updatecustomer.qfd): Updates an existing customer. It requires the customer records `wc_auth ID` and the updated information. (For details, see UpdateCustomer on page 338.)
- DeleteCustomer (deletecustomer.qfd): Marks the customer record as deleted in the database, but does not actually remove the record. This flow requires the records `wc_auth ID`. (For details, see DeleteCustomer on page 338.)
- UndeleteCustomer (undeletecustomer.qfd): Restores a previously-deleted customer record. This flow requires the records `wc_auth ID`. (For details, see UndeleteCustomer on page 339.)
- GetAuthenticatedCustomer (getauthenticatedcustomer.qfd): Authenticates the customer's user name and password. It returns the customer record if successful.
- GetCustomerList (getcustomerlist.qfd): Retrieves the list of customer records (both active and deleted) that match the specified criteria.

AddCustomer

When a new customer record is submitted, the AddCustomer flow checks to see whether a record can be added without a conflict. If it does, the flow returns an error and does not create the new record. (This means that two customers on the same tenant cannot share the same email address, even if their login names are different.)

For example, if the following customer's record already exists in the database:

- Login name: bob

- Email: bob@noname.com
- Tenant: DefaultTenant

then the following examples show how the AddCustomer flow would process three different Create Customer requests:

Case 1: New customer requests to be added with:

- Name: bob2
- Email: bob@noname.com
- Tenant: DefaultTenant

Result: The email and tenant are the same, so AddCustomer would fail with a "customer already exists" message.

Case 2: New customer requests to be added with:

- Name: bob
- Email: bob@noname.com
- Tenant: OtherTenant

Result: The tenants are different, so AddCustomer succeeds and a new customer record is added to the database.

Case 3: New customer requests to be added with:

- Name: bob3
- Email: bob3@noname.com
- Tenant: DefaultTenant

Result: The email addresses are different, so AddCustomer succeeds and a new customer record is added to the database.

UpdateCustomer

The UpdateCustomer flow contains no restrictions on updating customer information. Therefore, it is possible for a customer to change his or her email address to one that is the same as another customer.

Because Web Management maintains record consistency during the update operation, having a duplicate email address during update does not lead to any errors during processing.

DeleteCustomer

The DeleteCustomer flow sets the deletedFlag for the customer’s record to 1 (true). The actual customer information is not deleted from the database.

UndeleteCustomer

The UndeleteCustomer flow sets the deletedFlag for the customer's record to 0 (false). The flow does *not* check to see if the customer record's email address is the same as another customer's record already in the database.

Setting up the WebSchedule Callback feature

The WebSchedule Callback feature allows a customer to schedule when a specified agent at the contact center will place a telephone call to the customer. The customer schedules the call from the contact center's website.

When a customer completes the scheduled call form on the Scheduled Callback web page, the WebSchedule Callback server sends the request to the specified agent for a callback. The agent receives the callback request on the Avaya Agent client and returns the call to the customer at the requested time.

Note:
The WebSchedule Callback feature is only available on the Avaya Agent client. It is not supported on the Avaya Agent Web Client or IC systems running with Siebel integration.

Configuring WebSchedule Callback properties

The working hours of the contact center can be configured from the website properties. These properties provided as part of the Web Admin pages under Tenant Administration properties. The default values (open at 9:00, close at 18:00) can be modified for specifying the working hours of the contact center.

To modify the working hours of the contact center, set the following tenant properties to the desired times. (For details, see Customizing tenant website properties on page 330.)

Property name	Default value	Comments
callback.checkcallbacktime	TRUE	When set to TRUE, enables the WebSchedule Callback feature.
callback.contactcenteropentime	09:00	Time must be specified in 24-hour and xx.xx format only.
callback.contactcenterclosetime	18:00	Time must be specified in 24-hour and xx.xx format only.

Setting up Shared Browsing

By default, Shared Browsing is enabled for all chat sessions if the customer's browser can support it (for a list of supported browsers, see *IC Installation Planning and Prerequisites*).

Shared browsing provides the following features:

Customer Send Page: The customer can select **Send Page** on the chat client to automatically send the web page they are currently viewing to the agent.

To disable this feature, set the tenant property `chat.attributes.SendPageCaller` to "no" for the desired tenant and language. (For details, see Customizing tenant website properties on page 330.)

Agent Auto-Sync: If Auto-Sync is enabled, the current page shown in the Agent's browser is automatically loaded into the customer's browser as well. If an agent clicks on a hypertext link and loads a new page, that page is also loaded in the customer's browser. For details about configuring Auto-Sync, see *Avaya Agent User Guide*.

Collaborative Form-filling: When an agent and customer "sync" web pages (either through the Customer Send Page feature or the Agent Auto-Sync feature), all form elements on the customer and agent browsers will also synchronize. Changes to a form element (such as a field or a radio button) by one party will be reflected in the other party's browser.

Some web forms may need to be customized before they can be shared. You must test all forms you plan to share before attempting a live interaction with a customer.

Note:
Form-filling is supported only on the Internet Explorer browser.

Collaborative Form-filling

Collaborative Form-filling, also known as the Collaboration feature, is now incorporated in the HTML Chat client. This feature enables the customer and the agent to collaborate and fill the forms on Web pages that are pushed by either the customer or the agent.

After the call is escalated by the customer, a Verisign Certificate seeking the permission of the customer to access the system resources is displayed.

When the customer accepts the certificate, a new Internet Explorer browser window is displayed. This Internet Explorer browser window is the collaboration window that displays all the pushed pages and serves the purpose of form-filling.

Collaborative Form-filling works only when the customer collaboration browser and the agent collaboration browser are on the same URL, and Web pages on both browsers have the same page layout. During collaborative form-filling, browser session, cookies and authentication information is not shared.

Collaborative Form-filling is possible for the following HTML elements:

- Text box
- Radio button
- Check box
- Drop-down list
- Text Area

Note:
These HTML elements are supported only if they are inside a HTML form. An ID tag is mandatory for the fields in the form that is shared as part of collaborative form-filling.

Collaborative Form-filling is supported under the following scenarios:

- If the HTML page uses a form to post data onto the server.
- When the HTML page is a Static page. A Static page does not use any background scripts and events that dynamically change the layout of the page.
- Form-filling is supported only on the Internet Explorer browser.

Collaborative Form-filling is not supported on pages that:

- dynamically get updated by scripts or events.
- dynamically insert elements into the form or use some dynamic style sheets to format the form on the page.

Using the DataWake feature

The DataWake feature uses a web server plug-in that filters requests from customer browsers using rules specified in Web Management DataWake Administration. Each filter contains one or more search terms, called regular expressions, which are used to find specific web addresses that have been accessed by customers within a recent period of time. When pages that match these regular expressions are accessed by customers, the “hits” are recorded to the DataWake table, along with the name of the customer and other information. Agents can see this information and use it in any way they have been instructed, including clicking buttons that have been programmed with specific actions.

The process of setting up a DataWake mostly involves creating one or more filters using regular expressions (search terms). When you upload the filters to the web server, Web Management can then track an agent’s or a customer’s visits to any web pages that match the filter criteria.

This section contains the following topics:

- Filters and regular expressions on page 342
- Ripple regular expressions on page 342
- Setting up filters on multiple web servers on page 342
- Syntax for regular and ripple expressions on page 344

Filters and regular expressions

Each filter contains two levels of regular expressions: tenant regular expressions and associated ripple regular expressions. The DataWake feature uses tenant regular expressions to determine the tenancy of the browser request. Once the tenancy has been determined, it uses the ripple expressions to determine whether the request is written to the database and how the request is classified in the database.

When a tenant regular expression and any associated ripple regular expressions are found, meaning that a customer has accessed a monitored page, an entry is made in the DataWake table, along with the name of the customer, and the description and priority that has been entered for the regular expressions.

Because each filter can contain multiple regular expressions, all of which will monitor web traffic on a server, you only need one filter per web server.

Ripple regular expressions

You use ripple regular expressions to drill down to more specific information about what customers are viewing on the company's web site.

For example, if you set a tenant regular expression to search for the FAQ page, the ripple regular expression could search for certain topics in customers' searches of that FAQ page or if you set a tenant regular expression to search for the escalate page, the ripple regular expressions could indicate whether the customer requested a chat, fax, email, or callback.

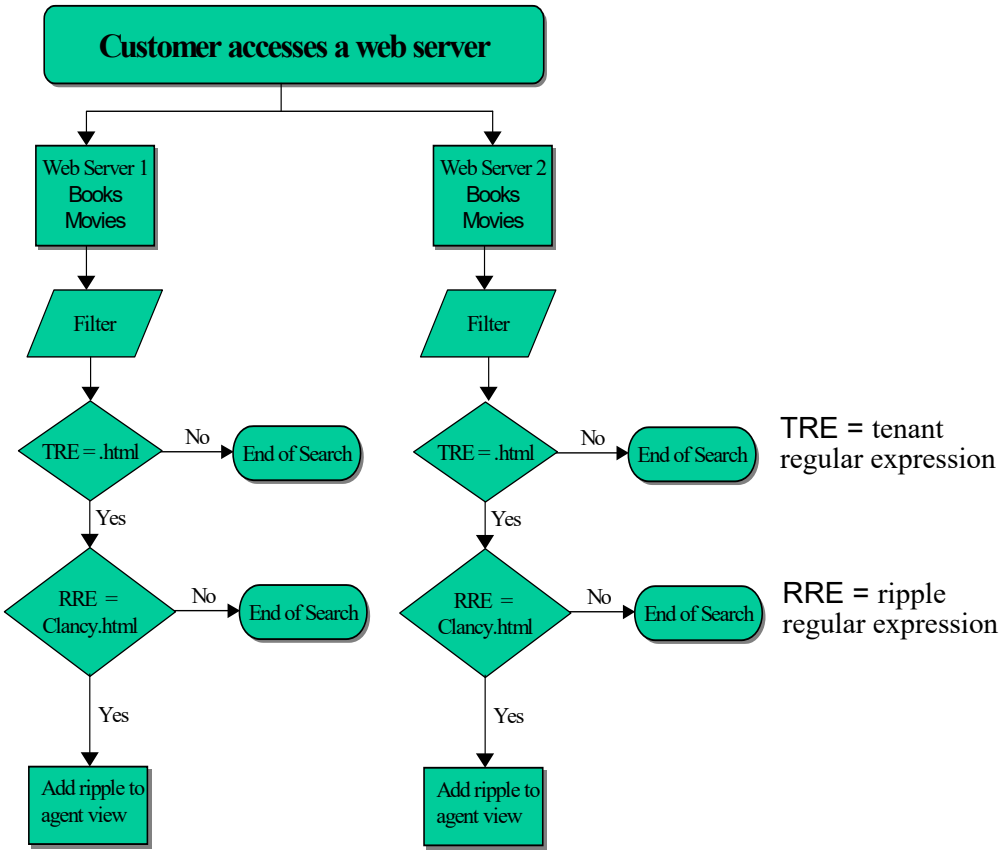
Ripple regular expressions also allow you to associate a priority, a description, and an expiration time to a web hit. For example, if Tenants A and B filter on the same tenant regular expression, `order.html`, but you want to place a higher priority on this file for Tenant A than for Tenant B, you can use a ripple regular expression to specify a different priority of the `order.html` regular expression for each tenant.

Ripple regular expressions also give you the ability to turn on or off logging customer hits to the database for each expression.

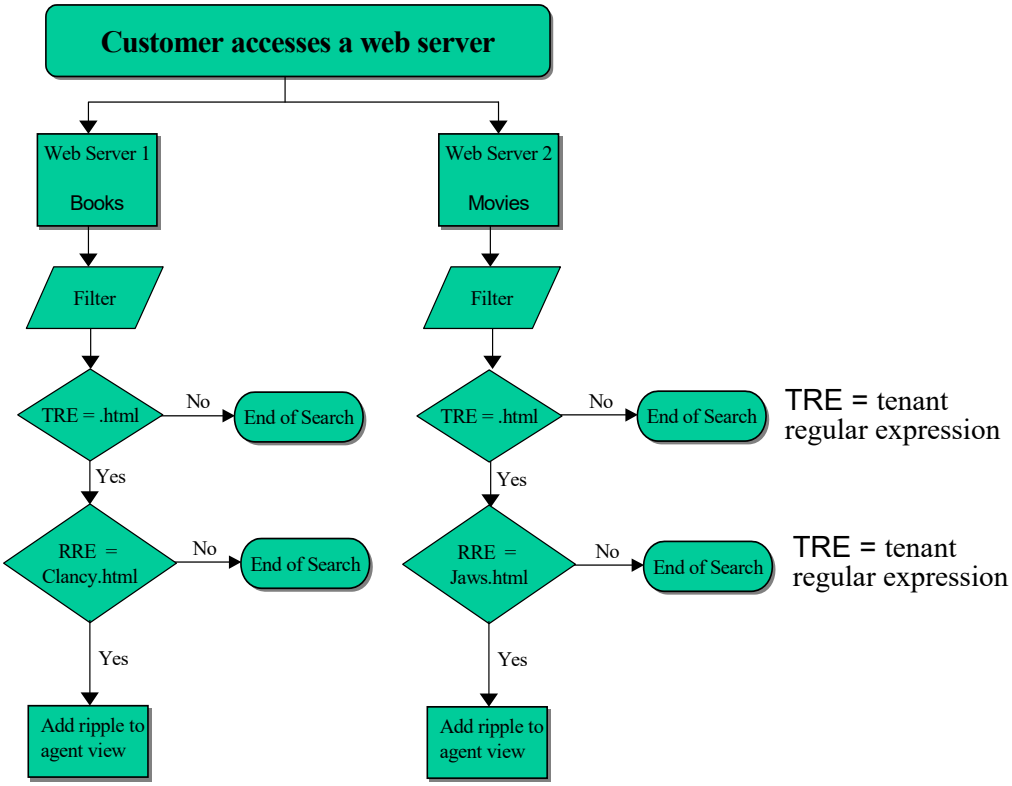
Setting up filters on multiple web servers

You can set up DataWake filters on multiple web servers in a variety of ways. The following examples describe two common methods.

The diagram below shows the DataWake filter setup with two different web servers hosting the same content, both having to do with “books” and “movies.” The administrator created two separate filters with the same filter information, tenant regular expressions and ripple regular expressions.



The next diagram shows the DataWake setup with the web content divided across two different servers, one server having content about “books” while the other server having content about “movies.” The administrator created a different filter for each web server, each filter pertaining to the web server’s specific topic. The ripple regular expression for books would find customer hits to the web page about Clancy, while the ripple regular expression for movies would find hits to the web page about Jaws.



Syntax for regular and ripple expressions

Tenant regular expressions and ripple regular expressions must follow certain syntax rules, which differ according to whether the filter is searching for single characters or multiple characters. Refer these rules if you want the filter to use special characters, wild cards, or more advanced methods of searching.

Single character regular expressions

The following table defines the syntax rules for creating single character regular expressions.

Rule	Example
Valid characters for regular expressions consist of alphanumeric characters. Special characters consist of the following symbols: + * ? . [ ] ^ $ \ You can also include the following reserved characters in a regular expression: , / @ = &	“a,” “b,” “c,”... or “1,” “2,” “3.”...
Any character that is *not* a special character matches itself.	Humpty will search for “Humpty”
You cannot use spaces in a regular expression.	
A backslash (\) followed by any special character matches the literal character itself.	*Humpty will search only for “*Humpty”
The period (.) matches any character except the new line character.	.umpty will search for “Humpty” or “Dumpty”
A set of characters enclosed in brackets is a one-character regular expression that matches any of the characters in that set. If the carat (^) is the *first* character in the set, the regular expression matches any character that is *not* in that set.	[ump] will search for a “u,” “m,” or “p” [^ump] will search for any characters except “u,” “m,” “p”
A range of characters enclosed in brackets (indicated with a dash) matches any character in that range.	[a-s] will search for any character from “a” to “s”

Multi-character regular expressions

The following table defines the syntax rules for creating multi-character regular expressions.

Rule	Example
A one-character regular expression followed by an asterisk (*) matches zero or more occurrences of the regular expression.	[a-d]* will search for zero or more characters for “a,” “b,” “c,” “d”
A one-character regular expression followed by a plus (+) sign matches one or more occurrences of the regular expression.	[a-d]+ will search for one or more characters for “a,” “b,” “c,” “d”
A regular expression followed by a question mark (?) matches zero to one occurrences of that regular expression.	xy?z will search for “xyz” or “xz”
The concatenation of regular expressions is a regular expression that matches the corresponding concatenation of strings.	[A-D][a-d]* will search for any string which consists of a single character "A", "B", "C", or "D" followed by zero or more characters with repeats allowed "a", "b", "c", or "d".

Setting up DataWake filters

DataWake filters communicate with the Attribute server to determine which customer hits on the server should be recorded.

By default, the IC Website Administration Tool creates a DataWake filter called “Main” on the installation machine. If you want to monitor other web servers, you need to make sure that the DataWake plug-in is properly installed and configured, and then create a DataWake filter on each of those servers.

CAUTION:
DataWake will not work without the special instructions contained in the default Main filter, even if you have created filters on other web servers. Therefore, you must not delete Main from the installation machine even if that’s not one of the web servers you want to watch.

When you create a new filter, you also need to define regular expressions associated with a specific tenant. You can add multiple regular expressions to the filter.

To create a new DataWake filter:

1. In Avaya IC Manager, select **Services** > **Web Response Unit**.

2. Select **Manage DataWake** under the **DataWake** section to open the **DataWake Management** page.
3. From the **Filter Management** section, select **New** to open the **Tenant Regular Expressions for Filter** page.
4. Under the **General Information** section, enter:
   - A name for the new filter in the **Filter Name** field.
   - The server name or IP address where the filter will be hosted in the **Host Name/IP** field.
5. Add the filter's regular or ripple regular expressions as desired. (For details, see Adding regular and ripple regular expressions on page 347.)
6. When all the tenant regular expressions are as you want them to be, select **Commit** to save the filter and expressions to the database.

   The IC Website Administration Tool redisplays the **DataWake Management** page.
7. In the **Update Filters** section, select **Update Filters** to send the changes to the server.

Adding regular and ripple regular expressions

You can add regular expression for a filter on the **Tenant Regular Expression for Filter** page, and then select an existing expression and add ripple regular expressions on the **Ripple Regular Expressions** page.

To add a regular expression:

1. In the **Filter Management** section of the **DataWake Management** page, select the filter for which you want to add a regular expression from the drop-down list.
2. Select **Maintain** to open the **Tenant Regular Expressions for Filter** page.
3. In the **Regular Expressions** section below the expressions table:
   a. Enter the tenant regular expression you want this filter to search for in the **Regular Expression** field. (Expressions can be up to 64 characters long. For the rules of syntax, see Syntax for regular and ripple expressions on page 344.)
   b. Select the tenant to which this expression applies from the **Tenant** drop-down list.
   c. Select **Add** to add the expression to the list of tenant regular expressions.

   Repeat this procedure for each regular expression you wish to add.
4. Select **Commit** to save the expressions to the database. The IC Website Administration Tool redisplays the **DataWake Management** page.
5. In the **Update Filters** section, select **Update Filters** to send the changes to the server.

To add a ripple regular expression:

1. In the expressions table on the **Tenant Regular Expressions for Filter** page, select the selection box next to the regular expression to which you want to add a ripple expression.

2. Select **Edit Ripples** to open the **Ripple Regular Expressions** page. The **Add** section appears below the ripple expression table.
3. You can specify:
   - The regular expression that you want to add in the **Regular Expression** field. You can enter between 1 and 64 alphanumeric characters.
   - The priority of the ripple regular expression in the **Priority** field. You can specify a number between 1 and 100, with 1 representing the highest level of priority and 100 the lowest. Agents can sort their views based on this priority.
   - A description for this ripple regular expression (such as escalation, browsing, ordering, or chat), in the **Description** field.
   - The amount of time, in seconds, that should elapse before this ripple is deleted from the DataWake system in the **Expiration (seconds)** field.
   - Whether you want this ripple logged to the database by selecting or clearing the **Log to DB** check box.

   Note:
   Any ripples that are logged to the database become part of the customer's DataWake record. Use the check box to turn logging on and off according to what your company determines to be currently significant. Only ripples with database logging turned on can be accessed by agents using the DataWake View feature.
4. Select **Add**.

   Repeat this procedure for all ripple expressions that you want to add.
5. Select **Done** to return to the Tenant Regular Expressions for Filter page.
6. Select **Commit** to save your changes to the database. The IC Website Administration Tool redisplays the **DataWake Management** page.
7. In the **Update Filters** section, select **Update Filters** to send the changed filters to the server.

Ordering expressions

The IC Website Administration Tool checks the expressions in the order in which they appear in the table. When the filter finds a match, it stops checking lower expressions in the table. Therefore, you should place your most specific expressions at the top.

For example, if you are using a regular expression to capture hits to the FAQ page, and another to capture customer searches on the FAQ page, you should put the search expression first in the table. Otherwise, the IC Website Administration Tool will record the hit to the FAQ and then stop, ignoring the more detailed search expression.

To set the order of regular expressions:

1. On the **DataWake Management** page, select the filter whose regular expressions you want to order and select **Maintain** to open the **Tenant Regular Expressions for Filter** page.
2. Select the selection box next to the regular expression you want to move.
3. Select **Move Up** or **Move Down** as appropriate.
4. Select **Commit** to save your changes to the database and return to the **DataWake Management** page.
5. Select **Update Filters** to send your changes to the server.

To set the order of ripple regular expressions:

1. On the **Tenant Regular Expressions for Filter** page, click the selection box next to the regular expression whose ripple expressions you want to order.
2. Select **Edit Ripples**.
3. Select the selection box next to the ripple regular expression you want to move.
4. Select **Move Up** or **Move Down** as appropriate.
5. Select **Done** to return to the **Tenant Regular Expressions for Filter** page.
6. Select **Commit** to save your changes to the database and return to the **DataWake Management** page.
7. Select **Update Filters** to send your changes to the server.

Modifying or deleting expressions

To delete or modify regular expressions in the regular expressions table or the ripple regular expressions table, you must first select an expression by clicking its selection box, then selecting **Remove** or **Edit**.

After you have made your changes, select **Commit** on the **Tenant Regular Expressions for Filter** page, then select **Update Filters** on the **DataWake Management** page.

Viewing DataWake records

The DataWake View page allows you or your agents view the DataWake record of anyone visiting one of your tenant's websites. The DataWake record is a list of the URLs on the tenant's site that a customer has visited during his or her browser session.

The **DataWake View** page has two sections:

- **Full DataWake History** lets you view the DataWake for any user
- **Agent's Current DataWake** lets you view your own browser session information.

Full DataWake history

To view the DataWake history:

1. In Avaya IC Manager, select **Services** > **Web Response Unit**.
2. From the **Self-Service** section, select **Self-Service Console**.
3. Select **DataWake View** to open the **DataWake Summary** page.
4. You can narrow your search results by entering any or all of the following information in the **Full DataWake History** section:
   - **User Name**: Enter a user name or leave this field blank to view the DataWake record for all users.

     If you enter a name in this field, the restrictions below apply to that user only. If you leave it blank but enter restrictions, then the results will show the restricted information for all users.
   - **Restrictions**: If you want to refine your view further, select one of the following restrictions:
     - **Start/End Date and Time**: View the DataWake generated only between the start and end dates and times.
     - **Last N Sessions**: View only the last N sessions.
     - **List of Session Ids**: View one or more specific session Ids (separate multiple Ids with commas).
5. Select **Display Full DataWake**.
6. Click on the DataWake record that you want to view. If you are prompted to log in, enter your current logon ID.

Viewing your own DataWake record

To view your own DataWake record:

1. Select **DataWake View** to open the **DataWake View** page.
2. In the **Agent's Current DataWake** section, select **Display Session** to view your current DataWake record.

Using the Email History feature

Email history is a feature in IC Website Administration tool to view the history of all email communications that an agent has with various customers.

In IC Administration tool, you can use the new Email History feature to first search the required email communications and then view the email message details for the required email communication.

This section contains the following topics:

- Enabling the Email History feature on page 351
- Accessing the Email History feature on page 353
- Viewing the Email History report on page 354
- Exporting the Email History report on page 355
- Copying the Email History report on page 356
- Searching an email message in the report on page 356
- Displaying the email message text on page 356
- Showing the number of records in the report on page 356
- Sorting the report list on page 357

Enabling the Email History feature

For the Email History feature in Avaya Interaction Center 7.3.3 release and later, there are certain changes made in the database schema, workflow, and the metadata properties of the IC Website Administration.

The changed database schema is available through the `ccq.adl` file, the workflow is available through the `webcenter.prj` project, and the metadata properties are available on the IC Website Administration site.

To enable the Email History option, you need to first update the `ccq.adl` file from the Database Designer application, upload the workflow to the database through Workflow Designer, and update the metadata properties on the IC Website Administration site.

This section contains the following topics:

- Updating the database schema on page 352
- Uploading the workflow to the database on page 352
- Settings the metadata properties on page 353

Updating the database schema

You need to update the database schema using the Avaya IC Database Designer application. For more information, see *IC Database Designer Application Reference*.

By default, the Avaya IC Design and Admin installer provides the `ccq735.adl` file. This file contains the configuration of the Email History feature.

To update the database schema:

1. On the Design and Admin system, go to the `design\ccq` directory.
2. Backup the existing `ccq.adl` file.
3. Rename the new `ccq733.adl` file to `ccq.adl`.
4. Add the custom configuration from your existing `ccq.adl` file to the new `ccq.adl` file.
   a. Open the new `ccq.adl` file and your backed up `ccq.adl` file in any editor.
   b. From the backed up `ccq.adl` file, copy all your custom configurations and paste them to the new `ccq.adl` file.
   c. Save the new `ccq.adl` file.
   d. Close both the `ccq.adl` file.
5. Reconfigure the database.
6. Generate the Windows application.

Uploading the workflow to the database

You need to upload the workflow to the database using Workflow Designer application. For more information, see *Avaya Workflow Designer User Guide*.

To update the workflow in Workflow Designer:

1. Start Workflow Designer application.
2. On the main menu bar, click **File** > **Open** Project.
3. Select the `webcenter.prj` file.
4. Specify the project settings.

5. Click **OK**.
6. Build the project.

   You must build the project to upload the workflow to the database so that the Workflow servers can access the workflow.
7. Restart the Workflow server or reload the workflow to the Workflow server.

Settings the metadata properties

To set the metadata properties on the IC Website administration page:

1. In a Web browser, navigate to the IC Website administration page.

   `http://<server_name>/website/admin/login.jsp`.
2. Enter the user name and password and click **Next** to login to the IC Website administration page.
3. Access the add metadata page.

   `http://<server_name>/website/admin/tenancy/addmd.jsp`
4. Add the following metadata property:
   - Metadata name = wruadmin.text.navbar.emailhistory
   - Default value = Email History
   - Select the **Tenant Property** option
5. Click **Add Metadata**.
6. Close the browser.

Accessing the Email History feature

An agent or supervisor can access the Email History feature to search the history of email communications with various customers. Agent can search the email history base on various parameters, such as date, EDUID, from address, to address, email subject, and so on.

To access the Email History feature:

1. In a browser, navigate to the IC Website administration page: `http://<server_name>/website/admin/login.jsp`.
2. Login to the IC Website administration page.
   - In the **Username** and **Password** fields, enter the valid user name and password.
   - Click **Next**.

   The system displays the Welcome page for Interaction Center Website Administration.
3. Click the **Select a Service** drop-down list and select **IC Web Self-Service**.

4. In the left pane, click **Web Self-Self Service console** link in the **Web Self-Service** section.
5. In the Web Self-Service list, click the **Email History** link to view the Email History Report page.

   On the Email History Report page, you can view the options to specify the criteria to search the particular email messages.

Viewing the Email History report

The Email History report page is setup for agents, supervisors, and administrators to view the history of the email communication between an agent and the customer.

To view the Email History report:

1. Access the **Email History Report** page. For more information, see Accessing the Email History feature on page 353.
2. In the fields, specify the appropriate values as explained in the following table:

Fields	Description
Date Range	The date range between which you want to view the email history. In the date range you can select the following option: • **Start Date**: The start date from which you want to view the email history. • **End Date**: The end date upto which you want to view the email history. • **Today**: The current date or the number of last days from the current date.
From Address	The email address of the person from whom you received the emails.
To Address	To email address of the person to whom you sent the emails.
Subject	The subject of the email message
Agent	The name of the agent for whom you want to see the email history.
Tracking No.	A unique tracking number that WebACD assigns to each email message.

3. After you specify the values in the fields, click the **Submit** button.

   The Email History report displays only the emails that match the specified criteria. The Email History report displays the information in a table with alternate rows in a color and with following columns:

Column	Description
Tracking No	The tracking number of the email message.
Create Date	The date when the email message is created.
From Address	The email address from whom the email is received.
To Address	The email address to whom the email message is sent.
Subject	The subject of the email message.
Current Status	The current status of the email message.
Special Status	The special status of the email message.
Agent	The name of the agent who has handled the email message.

Note:
To avoid database overload, the Email History report page displays only 300 email records for the specified search criteria. Also, for the emails with same EDU ID, the table displays the rows in same color. Rows with same color are easy to view the conversation thread if any transfers took place.

4. On the Email History report page, click the **Next** and **Previous** button to navigate to another pages of the report.

Exporting the Email History report

To export the Email History report:

1. On the Email History report page, click any of the following buttons:
   - **CSV**: The report is exported to a comma separate file with an extension .CSV.
   - **Excel**: The report is exported to an Excel file with extension .xls.
   - **PDF**: The report is exported to a PDF file with an extension .PDF
2. In the File Open dialog box, specify the appropriate file name and the folder.
3. Click **Save**.

Copying the Email History report

To copy the Email History report:

1. On the Email History report page, click the **Copy** button next to the **Search** field.

   The system copies the records from the table on current page.

Searching an email message in the report

After you generate a report, you can also search for a particular email message in the report.

To search an email message in the report:

1. Generate the Email History report.
2. On the Email History report page, enter the search string in the **Search** field.

   The system starts displaying the email messages that matches the text that you type in the Search field.

Displaying the email message text

When you generate the Email History report, you can view the list of emails that matches the specified criteria. From the list of emails, you can select particular emails to view the message in that email.

To display the email message:

1. Display the Email History report.
2. In the email messages list, select the check box corresponding to the email for which you want to view the message.
3. Click the **Get Message Text** button.

Note:
If you select multiple emails in the list, the messages for the selected emails are displayed one after another.

Showing the number of records in the report

When you generate the Email History report, the Email History report page displays 10 records. However, you can change that number to view more records on the page.

To show the number of records in the report:

1. On the Email History report page, click the **Show entries** drop-down list.
2. From the list, select the number of records that you want to view. On a page, you can view up to 100 records.

Sorting the report list

When you generate the Email History report, you can sort the report list according to the columns in the report.

To sort the report list:

1. In the report list, click the **Up** or **Down** arrow next to the column label.

   The blue color to the UP and Down arrow indicates by which column the report list is sorted and also indicates whether the report is sorted in ascending or descending order.

Using the Chat History feature

Chat history is a feature in IC Website Administration tool to view the history of all chat communications that an agent has with various customers.

In IC Administration tool, you can use the new Chat History feature to first search the required chat communications and then view the chat message details for the required chat communication.

This section contains the following topics:

- Enabling the Chat History feature on page 358
- Accessing the Chat History feature on page 359
- Viewing the Chat History report on page 360
- Exporting the Chat History report on page 361
- Copying the Email History report on page 362
- Searching a chat communication in the report on page 362
- Displaying the chat communication details on page 362
- Showing the number of records in the report on page 363
- Sorting the report list on page 363

Enabling the Chat History feature

For the Chat History feature in Avaya Interaction Center 7.3.3 release and later, there are certain changes made in the database schema, workflow, and the metadata properties of the IC Website Administration.

The changed database schema is available through the `ccq.adl` file, the workflow is available through the `webcenter.prj` project, and the metadata properties are available on the IC Website Administration site.

To enable the Chat History option, you need to first update the `ccq.adl` file from the Database Designer application, upload the workflow to the database through Workflow Designer, and update the metadata properties on the IC Website Administration site.

This section contains the following topics:

- Updating the database schema on page 358
- Uploading the workflow to the database on page 359
- Settings the metadata properties on page 359

Updating the database schema

You need to update the database schema using the Avaya IC Database Designer application. For more information, see *IC Database Designer Application Reference*.

By default, the Avaya IC Design and Admin installer provides the `ccq733.adl` file. This file contains the configuration of the Chat History feature.

To update the database schema:

1. On the Design and Admin system, go to the `design\ccq` directory.
2. Backup the existing `ccq.adl` file.
3. Rename the new `ccq733.adl` file to `ccq.adl`.
4. Add the custom configuration from your existing `ccq.adl` file to the new `ccq.adl` file.
   a. Open the new `ccq.adl` file and your backed up `ccq.adl` file in any editor.
   b. From the backed up `ccq.adl` file, copy all your custom configurations and paste them to the new `ccq.adl` file.
   c. Save the new `ccq.adl` file.
   d. Close both the `ccq.adl` file.
5. Reconfigure the database.
6. Generate the Windows application.

Uploading the workflow to the database

You need to upload the workflow to the database using Workflow Designer application. For more information, see *Avaya Workflow Designer User Guide*.

To update the workflow in Workflow Designer:

1. Start Workflow Designer application.
2. On the main menu bar, click **File** > **Open** Project.
3. Select the `webcenter.prj` file.
4. Specify the project settings.
5. Click **OK**.
6. Build the project.

   You must build the project to upload the workflow to the database so that the Workflow servers can access the workflow.
7. Restart the Workflow server or reload the workflow to the Workflow server.

Settings the metadata properties

To set the metadata properties on the IC Website administration page:

1. In a Web browser, navigate to the IC Website administration page.

   `http://<server_name>/website/admin/login.jsp`.
2. Enter the user name and password and click **Next** to login to the IC Website administration page.
3. Access the add metadata page.

   `http://<server_name>/website/admin/tenancy/addmd.jsp`
4. Add the following metadata property:
   - Metadata name = wruadmin.text.navbar.chathistory
   - Default value = Chat History
   - Select the **Tenant Property** option
5. Click **Add Metadata**.
6. Close the browser.

Accessing the Chat History feature

An agent or supervisor can access the Chat History feature to search the history of chat communications with various customers. Agent can search the chat history based on various parameters, such as date, EDU ID, customer name, chat queue, agent name, exit reason, and so on.

To access the Chat History feature:

1. In a browser, navigate to the IC Website administration page: `http://<server_name>/website/admin/login.jsp`.
2. Login to the IC Website administration page.
   - In the **Username** and **Password** fields, enter the valid user name and password.
   - Click **Next**.

   The system displays the Welcome page for Interaction Center Website Administration.
3. Click the **Select a Service** drop-down list and select **IC Web Self-Service**.
4. In the left pane, click **Web Self-Self Service console** link in the **Web Self-Service** section.
5. In the Web Self-Service list, click the **Chat History** link to view the Chat History Report page.

   On the Chat History Report page, you can view the options to specify the criteria to search the particular chat messages.

Viewing the Chat History report

The Chat History report page is setup for agents, supervisors, and administrators to view the history of the chat communication between an agent and the customer.

To view the Chat History report:

1. Access the **Chat History Report** page. For more information, see Accessing the Chat History feature on page 359.
2. In the fields, specify the appropriate values as explained in the following table:

Fields	Description
Date Range	The date range between which you want to view the chat history. In the date range you can select the following option: • **Start Date**: The start date from which you want to view the chat history. • **End Date**: The end date upto which you want to view the chat history. • **Today**: The current date or the number of last days from the current date.
Customer Name	The name of the customer with whom the chat communication is performed.
Chat queue	The queue name in which the chat request was added.
Agent	The name of the agent for whom you want to see the chat history.
Exit Reason	The reason of the chat communication exit.

Fields	Description
Task ID	A unique ID that represents the chat contact.
EDU ID	A unique ID that represents the contact as a task for the routing engine to route the call to an agent.

3. After you specify the values in the fields, click the **Submit** button.

   The Chat History report displays only the chat communications that match the specified criteria. The Chat History report displays the information in a table with alternate rows in a color and with following columns:

Column	Description
EDU ID	A unique ID that represents the chat contact.
Task ID	A unique ID that represents the contact as a task for the routing engine to route the call to an agent.
Start Time	The start time of the chat communication.
Chat Queue	The queue name in which the chat request is added.
Agent Name	The name of the agent who handled the chat request.
Customer Name	The name of the customer who requested the chat communication.
Resolution	The resolution of the chat communication request.

Note:
To avoid database overload, the Chat History report page displays only 300 chat records for the specified search criteria. Also, for the chat communications with same EDU ID, the table displays the rows in same color. Rows with same color are easy to view the conversation thread if any transfers took place.

4. On the Chat History report page, click the **Next** and **Previous** button to navigate to another pages of the report.

Exporting the Chat History report

To export the Chat History report:

1. On the Email History report page, click any of the following buttons:
   - **CSV**: The report is exported to a comma separate file with an extension .CSV.
   - **Excel**: The report is exported to an Excel file with extension .xls.
   - **PDF**: The report is exported to a PDF file with an extension .PDF

2. In the File Open dialog box, specify the appropriate file name and the folder.
3. Click **Save**.

Copying the Email History report

To copy the Chat History report:

1. On the Chat History report page, click the **Copy** button next to the **Search** field.

   The system copies the records from the table on current page.

Searching a chat communication in the report

After you generate a report, you can also search for a particular chat communication in the report.

To search a chat communication in the report:

1. Generate the Chat History report.
2. On the Chat History report page, enter the search string in the **Search** field.

   The system starts displaying the chat communications that matches the text that you type in the Search field.

Displaying the chat communication details

When you generate the Chat History report, you can view the list of chat communications that matches the specified criteria. From the list of chat communications, you can select particular chat communication and view the details of that communication.

To display the chat communication details:

1. Display the Chat History report.
2. In the chat communication list, select the check box corresponding to the chat communication for which you want to view the message.
3. Click the **Get Message Text** button.

Note:
If you select multiple chat communications in the list, the details of the selected chat communications are displayed one after another.

Showing the number of records in the report

When you generate the Chat History report, the Chat History report page displays 10 records. However, you can change that number to view more records on the page.

To show the number of records in the report:

1. On the Chat History report page, click the **Show entries** drop-down list.
2. From the list, select the number of records that you want to view. On a page, you can view up to 100 records.

Sorting the report list

When you generate the Chat History report, you can sort the report list according to the columns in the report.

To sort the report list:

1. In the report list, click the **Up** or **Down** arrow next to the column label.

The blue color to the UP and Down arrow indicates by which column the report list is sorted and also indicates whether the report is sorted in ascending or descending order.

Chapter 15: Properties

Properties are behavior and appearance options that you can define in Avaya IC Manager and then assign to **IC** (the top-level Avaya IC environment entity), tenants, workgroups, or agents. They define the colors that are displayed on the workstation, the shape of the buttons, and the behavior of the agent's applications.

Avaya IC Manager stores the properties in the database so that Avaya IC applications, can retrieve the property settings. Storing properties in the database also means that no matter what machine an agent uses, Avaya Agent always looks and behaves the same way.

Properties are inherited by Avaya IC entities (tenants, workgroups, agents) as they flow down an inheritance path from parent to child entities. When you assign agents to workgroups, you can specify the order of inheritance. This order controls what property value Avaya IC Manager uses if an entity ends up inheriting multiple values for the same property. (For details, see Property inheritance on page 365.)

Properties can be changed by the agent if you designate them as customizable. For example, you can let agents configure the color of alert messages based on their level of severity. For more information, see Creating properties on page 370.)

Avaya IC provides a basic set of properties out-of-the-box. You can create new properties or expand the attributes of existing properties to make the application fit your needs. For additional information and descriptions of the properties that are provided with Avaya IC, see Appendix E: Property descriptions on page 570.

Note:

Before you can declare and assign new properties, you must create a Avaya IC organization to which the properties can be assigned. For instructions on creating tenants and workgroups, see Chapter 10: Workgroups and tenants on page 240. For detailed information on assigning properties directly to agents, see Chapter 9: Managing Agents on page 214.

This section contains the following topics:

- Property inheritance on page 365
- Setting up properties and property sections on page 369
- Changing properties on page 372
- Deleting properties on page 374

Property inheritance

Properties can be assigned to **IC**, tenants, workgroups, and agents. These properties can be inherited by their member entities to create a consistent work environment. For example, you might want all of the agents in a particular workgroup to have access to the same desktop applications.

When you assign one entity (tenant, workgroup, agent) to another, the top-level entity becomes the parent of the lower-level entity. The lower-level entity then inherits all of the parent entity's properties, along with any properties the parent entity may have inherited.

For example, if you assign the property `OldStyleButtons = False` to the **IC** entity, then assign the workgroup Loans to the **IC** entity, any agent assigned to the Loans workgroup automatically inherits the property `OldStyleButtons = False`.

You can designate property inheritance as cumulative or non-cumulative when you declare the property. If a property is cumulative, then multiple instances of the property are permitted, and the system remembers all of the possible settings for each agent. (For details, see Cumulative property inheritance on page 365.) If a property is non-cumulative, Avaya IC Manager collects all of the settings for each property that are either assigned directly to the agent or inherited from the entities that the agent is assigned to. Avaya IC Manager then decides which setting to use based on the inheritance rules described in Non-cumulative property inheritance on page 366.

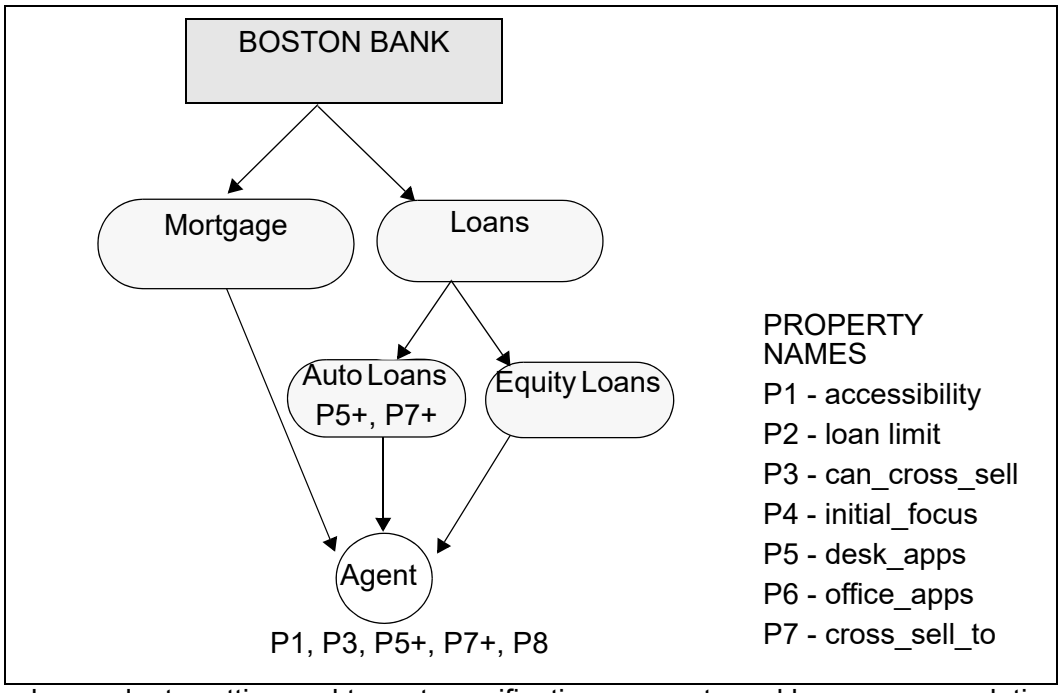
If agents are assigned to multiple workgroups, they inherit properties from each workgroup and potentially from each entity to which the workgroups are assigned. Avaya IC Manager resolves conflicts arising from duplicate properties based on the order defined for the agent's workgroups. For an example of a property inheritance scheme involving multiple workgroups, see Sample inheritance scheme on page 367.

Note:
If a contact does not have an associated tenant, then Avaya IC ignores any tenant-based properties. Voice contacts, for example, are never associated with a tenant, so Avaya IC never applies tenant properties to them.

Cumulative property inheritance

When a property's inheritance is cumulative, multiple occurrences of the property are permitted. The cumulative property values that are assigned to agents through membership in tenants or workgroups are collected and accumulated.

For example, the **desk_apps** property can be defined as cumulative to give agents working with Auto Loans both the Blue Book application and the Loan Calculator application. In the following diagram, the **desk_apps** (P5+) property is directly assigned to the agent. It is also inherited by the agent through the Auto Loans workgroup.

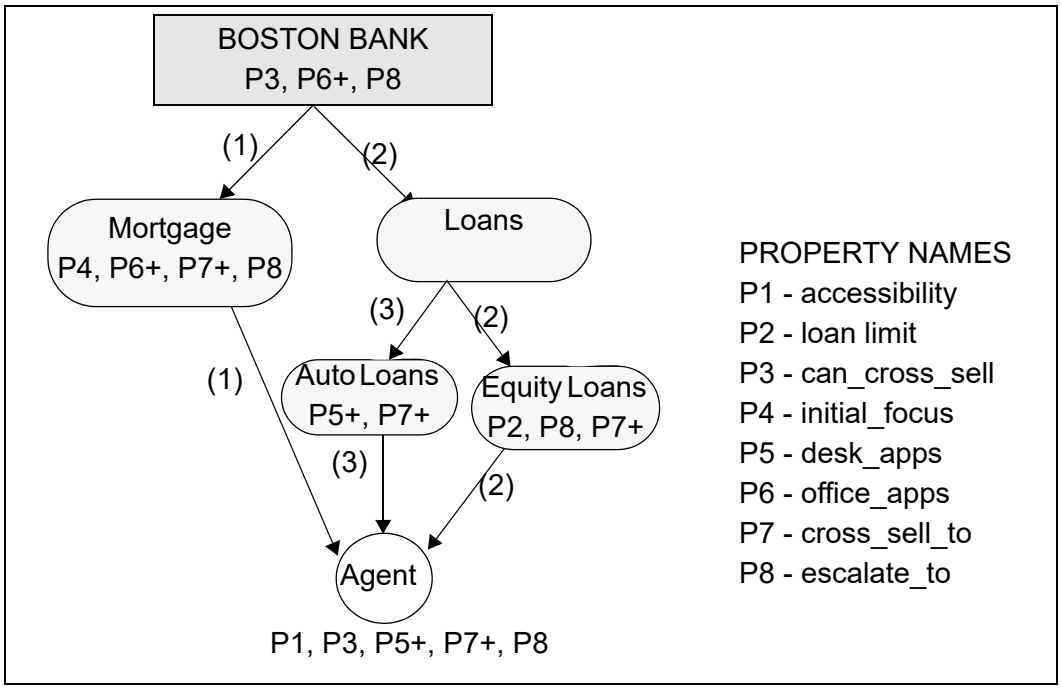


The override by descendants setting and tenant specifications are not used because, cumulative property values already exist.

Non-cumulative property inheritance

When a property's inheritance is non-cumulative, Avaya IC Manager uses the inheritance override settings. After locating all occurrences of the property, each one is evaluated by its property setting. The effective setting is established by reading each occurrence as it flows down the hierarchal structure via the workgroup path. The inheritance order is determined by agent's primary workgroup path, followed by the secondary workgroup path, and so on.

In the following example, the agent inherits different values for the **escalate_to** (P8) property. The property value is "Joe" for the property that is inherited from the Boston Bank tenant through the Mortgages workgroup. The property value is "Joan" for the property inherited through the Equity Loans workgroups. The conflict is resolved by assigning the value "Joe" to the agent because it is inherited through the **primary** (1) workgroup path.



If the override by descendants setting for the property is enabled when you assign the property to an entity, the next available occurrence is read until the system finds an occurrence with a disabled override by descendants attribute to determine the inheritance setting for the property.

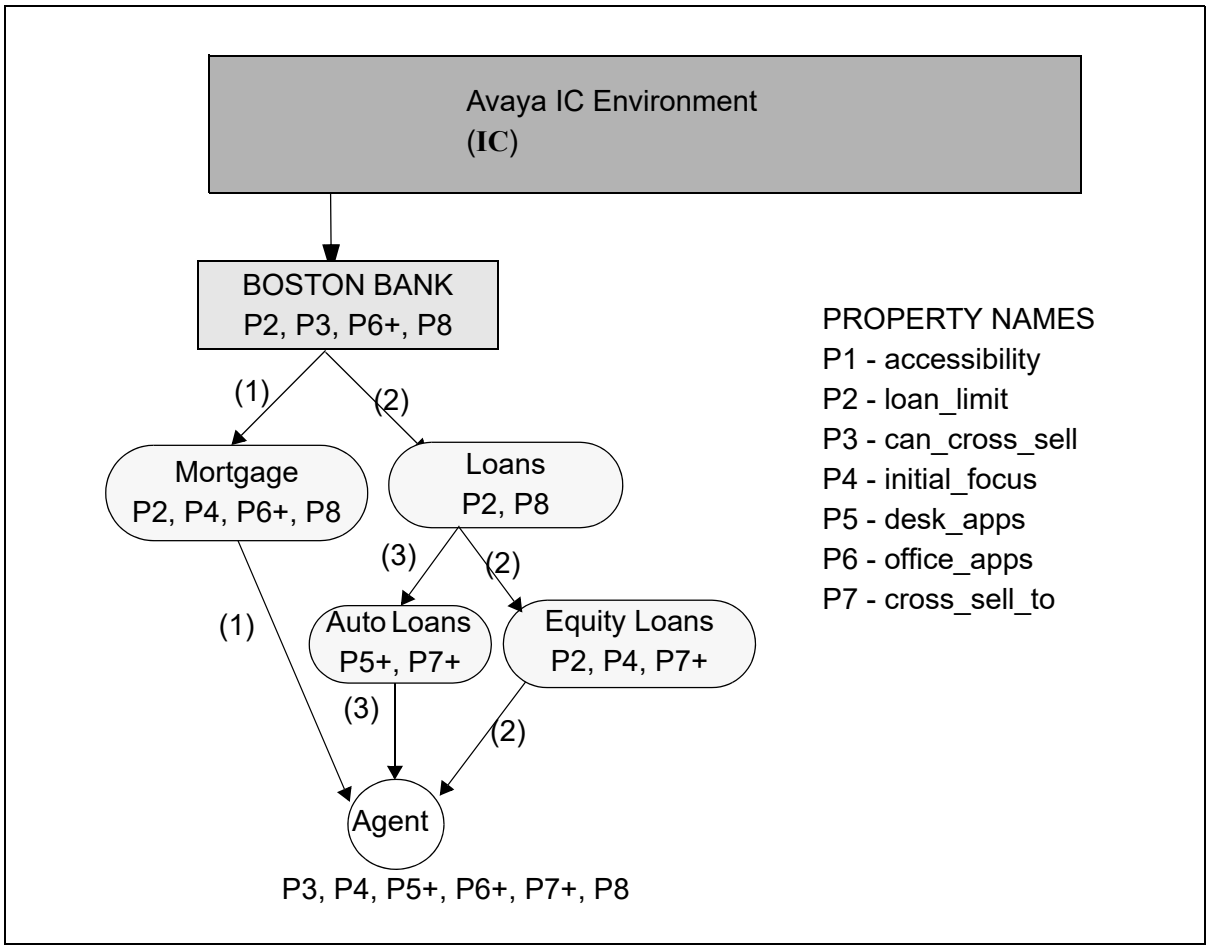
Note:

If Avaya IC does not find a property occurrence with a disabled override by descendants setting, the effective property setting is either that of the agent or the lowest level property occurrence.

Sample inheritance scheme

In the following example, properties are assigned to the Boston Bank tenant. They are inherited by the workgroups assigned to Boston Bank. The diagram illustrates the properties assigned to each of the entities in the Boston Bank tenant and the order of property inheritance for them.

Properties P5, P6, and P7 are cumulative (+) properties.



In this example there are properties assigned to the tenant for Boston Bank. The values for these properties flow down the tree structure in the designated order and they are either accumulated (cumulative) or replaced (non-cumulative).

- Boston Bank has properties that set the loan limit (P2), enable cross selling (P3), determine the office application (P6+) to be used, and determine that escalation of issues path (P8). The office application property (P6+) is a cumulative property, therefore agents can inherit more than one office application.
- Mortgages has properties that set the loan limit (P2), select the first focus to be displayed when the application is started (P4), and determine which office application (P6+) is used. It also has a property that defines to whom to escalate issues (P8). The office application property (P6+) is inherited from Boston Bank. For this example, the loan limit property for Mortgages is set at $750,000.
- Loans has non-cumulative properties that set the loan limit (P2) and specify to whom to escalate issues (P8). As a non-cumulative property, this value of P8 overrides the Boston Bank value for P8.

- Auto Loans has cumulative properties that determine the desktop applications (P5+) to be used and to whom the agent can cross sell (P7+). For this example, the value of the desktop application property (P5+) is Loan Calculator.
- Equity Loans has non-cumulative properties set the loan limit for the workgroup (P2). It also inherits a property that determines the first focus to be displayed when the application is started (P4) and the cumulative property that defines to whom the agent can cross sell (P7+). For this example, the loan limit property for Equity Loans is $50,000.

What Happened?

- The agent inherited all of the properties through the primary workgroup path (1), which are P3, P4, P5+, P6+, P7+, and P8.
- The property that defines the desktop application (P5+) as Blue Book is directly assigned to the agent.
- The agent has accumulated both the Loan Calculator, through inheritance, and Blue Book desktop, through direct assignment, applications.
- The agent inherits the loan limit value (P2) in the following order:
  - Primary workgroup path (1) = Mortgages, $750,000.
  - Secondary workgroup path (2) = Equity Loans, $50,000.

Setting up properties and property sections

Before assigning new properties to Avaya IC entities, you must declare them with a name and description, then group them into property sections. Property sections are functional units used to organize properties in Avaya IC Manager. Multiple properties can have the same name as long as they reside in different property sections.

Property values can be predefined (a user assigning a property to an entity must select from a given set of property values), or set ‘on the fly’ (a user assigning a property to an entity can enter a free-form property value).

Avaya IC Manager is pre-configured with generic property sections and types, which are described in Appendix E: Property descriptions on page 570. The Property Type Editor lets you create additional sections and properties and assign them to **IC**, tenants, workgroups, and agents.

To set up property sections and properties:

1. Create the property sections under which you want to group the new properties. (For details, see Creating property sections on page 370.)
2. Create the properties you want to use within each property section. (For details, see Creating properties on page 370.)

Creating property sections

Property sections are functional units that are used to organize and manage large numbers of properties in Avaya IC Manager. Multiple properties can have the same name as long as they reside in different property sections.

To create a new property section:

1. Select **Tools > Property Declarations**.

   Avaya IC Manager displays the **Property Declarations** dialog.

2. Select **New** below the **Property Section** pane.

   Avaya IC Manager displays the **Create Section** dialog box.

3. Enter the name of the section and its description in the appropriate fields. Click **OK**.

   Tip:
   Avaya IC Manager displays the description in other areas of Avaya IC where property assignment is done. You should make sure your description clearly defines the property so that it will make sense later.

Repeat this procedure for each property section you want to create. Avaya IC Manager displays the property section names and descriptions in the appropriate fields on Property Section pane.

After you have created your property sections, you can add properties to them. For details, see Creating properties on page 370.

Creating properties

After you have created your property sections, you can create properties to go with those sections. To do so:

1. Select **Tools > Property Declarations**.

   Avaya IC Manager displays the **Property Declarations** dialog.

2. In the **Property Section** pane, select the name of the section under which the new property should be grouped.

3. In the right-hand pane, select **New**.

   Avaya IC Manager displays the **Declare Property** dialog box.

4. Enter the property's name and description in the appropriate fields. The property name must be unique within the section.

5. Select the **Property Datatype** drop-down list and select the datatype that is appropriate for the property that you are creating. You can select from string, boolean, integer, longtext, or datetime. The datatype restricts the values that can be assigned to the property.

6. Select **OK** to place the new property to the designated section and close the **Create Property Type** dialog.
7. On the **Property Declaration** dialog's **Settings** tab, you can specify the following property settings:
   - If the property is required, select the **A value is required** check box. This means the property must exist and have a value. The **A value is required** check box is enabled only if you have selected any property in the property section right-hand side box.
   - If agents can enter a property value by typing in a text field as well as selecting from a pick list, select the **Allow typed-in values** check box.
   - If this property is cumulative, select the **Concatenate inherited values** check box. This lets you add this property to multiple entities as the inheritance flows down through the designated workgroup order. (For more information, see Cumulative property inheritance on page 365.)
8. In the **Applicable Property Levels** group, select the Avaya IC entities that can use the new property. If you specify multiple entities, then Avaya IC uses inheritance rules to determine what setting to apply when an agent logs in. (For details, see Property inheritance on page 365.) If you want:
   - all entities within the Avaya IC system to use this property, select **IC (Root Node)**.
   - specific tenants, their assigned workgroups, and the agents belonging to those workgroups to use this property, select **Tenants**.
   - specific workgroups and the agents assigned to those workgroups to use this property, select **Workgroups**.
   - specific agents to use this property, select **Individual Agents**.
9. If you want to assign the allowable values for this property:
   a. Select the **Values** tab.
   b. Select **New** to display the **Declare Value** dialog.
   c. Enter the name and description of the value in the appropriate fields.
   d. Select **OK** to return to the **Values** tab.

   Repeat this procedure for each value you want to enter.
10. Select **OK** to apply the settings to the property and close the **Property Declarations** dialog box.
11. After you have created your properties, assign them to the appropriate Avaya IC entities and set the value that Avaya IC should use for each one. For instructions on assigning properties to **IC**, tenants, or workgroups, see Assigning tenant and workgroup properties on page 248. For instructions on assigning properties directly to agents, see Assigning agent properties on page 230.

Tip:
You cannot select the value that Avaya IC should use for a particular property until you assign it to an entity. Therefore, if you create a property but do not assign it to anything, then that property has no effect on the Avaya IC system.

Changing properties

Avaya IC Manager lets you modify the following property attributes using the **Property Type Editor**:

- Names and descriptions of existing property sections
- Names and datatypes of existing properties
- Attributes assigned to existing properties
- Values assigned to existing properties

Note:
If you change property information, any agents linked to that property must log out of Avaya IC and then log back in again before the changes will take effect.

Changing property sections

To change the name and description of a property section:

1. Select the property section name in the **Property Section** pane.
2. Select **Edit** below the **Property Section** pane.

   Avaya IC Manager displays the **Edit Section** dialog.
3. Enter your changes in the **Name** and **Description** fields.
4. Select **OK** to save your changes.

Changing property names and datatypes

To change a property's name and datatype:

1. Select the property name in the **Properties** pane.
2. Select **Edit** below the **Properties** pane.

   Avaya IC Manager displays the **Edit Property Type** dialog.
3. Make your changes to the name, description, and datatype of the property.

4. Select **OK** to save these changes.

Note:
You cannot change the datatype of a property if there are values and instances of the property that require the datatype.

Changing property settings

To change property settings:

1. Select the name of the property in the **Properties** pane.
2. Select the **Settings** tab.

   Avaya IC Manager displays the attributes that are assigned to the property.
3. Select or clear the settings you want to change:
   a. **A value is required**. The property must exist and have a value.
   b. **Allow typed-in values**. The user can enter values for the property by typing them into a text field as well as selecting them from a pick list.
   c. **Concatenate inherited values**. Makes this property cumulative and allows multiple occurrences of this property with no inheritance override by the system. Cumulative values for a property are concatenated together in a pipe ("|") separated list. (For details, see Cumulative property inheritance on page 365.)
4. In the **Applicable Property Levels** pane, select the Avaya IC entities that are authorized to use this property. Clear those entities that are *not* authorized to use the properties.
5. Select **OK** to save these property settings.

Changing property values

To change property values:

1. Select the property section in the **Property Section** pane.
2. Select the property type in the **Properties** pane.
3. Select the **Values** tab.
4. Select **Edit** to display the **Edit Property Type** dialog.
5. Enter your changes in the **Name** and **Description** fields.
6. Select **OK**.

Deleting properties

You can delete property sections, property types, and property values from the system using the Property Type Editor.

Note:
All instances of a property must be deleted before you can delete the property itself. If you change or remove a value from a property, that could invalidate existing instances that use the value. Similarly, you cannot delete a property section if there are properties assigned to it. Typically, the Administrator of the system is responsible for resolving any conflicts.

Deleting property sections

To delete property sections:

1. Select the property section name in the **Property Section** pane.
2. Select **Delete** below the pane.

   Avaya IC Manager removes the section from the **Property Section** pane.
3. Select **OK** to delete.

Deleting properties

To delete properties:

1. Select the property name in the **Properties** pane.
2. Select **Delete** below the pane.

   Avaya IC Manager removes the property from the **Properties** pane.
3. Select **OK** to delete.

Deleting property values

To delete property values:

1. Select the property in the **Properties** pane.
2. Select the **Values** tab.
3. Select the value that you want to delete.

4. Select **Delete**.

   Avaya IC Manager removes the name and description from the **Create Property Value** dialog.

5. Select **OK** to delete.

Chapter 16: Devices and queues

Avaya Interaction Center (Avaya IC) lets agents receive and handle contacts over multiple media channels: text chat, telephony calls, email, VoIP (Voice over IP), and web based e-commerce. You need to create at least one queue for each of the different media channels that your company will be using. In addition to these queues, you can create a voice parking entity that serves as a waiting area for Telephony contacts until Avaya IC can put them into the appropriate queue.

Once you have created your queues, you can group them together through workgroups. Unless you are using Business Advocate for contact routing, Avaya IC uses workgroups to make routing decisions, so you need to construct your workgroups carefully. (For details, see Workgroups on page 242.)

Important:
Business Advocate does not use the queues or workgroups that are created in Avaya IC Manager for routing. You do not have to create the Voice/Chat/Email queues for Business Advocate to route contacts. For Business Advocate, the concept of IC queues and workgroups is replaced by Service Class. For more information, see *IC Business Advocate Configuration and Administration*.

You can also group queues together logically by creating a virtual queue. Virtual queues let you:

- Refer to a group of queues by a single name in a workflow or IC Script.
- Group Business Advocate services classes together geographically.
- Monitor a group of queues that cross site boundaries. It does not matter where these queues exist geographically.

You can create the following devices in Avaya IC Manager:

Voice Queue: A Telephony queue.

Note:
Avaya IC Manager does not instantiate or configure third party ACD queues and Avaya Communication Manager vectors.

Advocate Voice Parking Device: A vector/VDN where telephony contacts can be held until an agent becomes available. (This feature is only available if you are using Business Advocate.)

Chat Queue: A queue for text-based chat tasks.

Email Queue: A queue that handles email contacts. This queue requires that an associated mail account be configured on the system, a ccq database, and IC Repository database. For more information on setting up mail accounts, see Email accounts on page 111.

Virtual Queue: A collection of queues or Business Advocate service classes that can be referred to by a single name in a workflow or IC Script.

You can use the Device Manager to view, add, and modify the devices in the Avaya IC environment. However, in most cases, Avaya IC Manager cannot directly manage these queues. For more information, contact your switch administrator.

To access the Device Manager, select the Device tab in the Avaya IC Manager window. The left pane lists the devices, media types, and virtual queues that are available in Avaya IC. To view:

- Both queues and parking entities, expand the Devices category.
- All media channel queues sorted by channel type, expand the All Media category.
- All virtual queues, expand the Virtual Queues category.
- The details for a particular queue, select the queue name.

The right pane lists the following information:

Field Name	Description
ID	The media channel specific id of the queue. This parameter is used by the Chat, Email, and Voice channels. • For the Chat channel, it shows the tenant in default@default format. • For the Email channel, it shows the tenant in default@default format. • For the Voice channel, the queue id is based on the switch. For details, see Creating devices on page 378. The Queue ID must be unique for a media channel in a specific site.
Site	The geographic grouping that the queue belongs to. In a non-Business Advocate installation, Avaya IC uses this information when it makes routing decisions. In addition, you can assign particular servers to monitor all of the queues at a specific site. For details, see Managing sites on page 37. For details about the site to use with the voice channel, see Creating devices on page 378.
In a non-Business Advocate installation, the following fields are reserved for use by Avaya IC routing services. This information should be consistent with the ACD.	
ACD Name	The name of the associated ACD. This is only enabled for voice queues.
Media	The media type (Chat, Voice, or Email) used by the device. This field is automatically set by Avaya IC Manager based on the type of device you are creating.
Priority	The priority level assigned to the queue. This is a numeric value that the administrator creates for the contact center. It can be 1 for the highest priority down to 10 for the lowest.

Field Name	Description
Service Level	The interval in seconds in which a queued contact should be assigned to an agent on the system. This is a time period value that varies across the media channels. The default is 00:00:00, set the interval to a time period that is appropriate for your site.
Minimum Agents	The fewest number of agents that should be assigned to the queue.
Tenant	The tenant to which the device is assigned. (Tenants are not applicable to voice queues.) This field does not apply to Business Advocate installations.

You can sort the list of devices by clicking on a column header. Use Shift+click to sort the list in descending order. To automatically sort the list by the first column, select **Device > Auto Sort**. When you select a media type, Avaya IC Manager sorts the corresponding queues.

You can change the size of the columns by clicking between column headings and dragging the black line to the desired size.

When you first display the Device Manager, no category is selected in the left pane, so there are no devices listed. You can change this default behavior by selecting **Device > Auto Load**. If you select **Auto Load**, Avaya IC Manager automatically selects the Devices category when it displays the Device Manager.

This section contains the following topics:

- Creating devices on page 378
- Creating virtual queues on page 384
- Changing device information on page 385
- Deleting devices on page 386

Creating devices

The Avaya IC database stores various pieces of information about devices, such as their name, type, and configuration settings. This information must be added to the directory to create the device on the system. The devices described in this section are not used by Business Advocate with the exception of Advocate Parking Devices and Virtual Queues which are described in *IC Business Advocate Configuration and Administration*.

Note:
The TSQS may timeout in a failover situation if there are more than 500 queues defined on the system. For details, see *IC Telephony Connectors Programmer Guide*.

To add a device to Avaya IC:

1. In Avaya IC Manager, select the **Device** tab.
2. Select **Device > New Device**.
3. Select the type of queue that you want to create:
   - **Voice Queue** for a Telephony queue, Avaya Communication Manager VDN that holds incoming calls.
   - **Advocate Voice Parking Device** for a holding area for Telephony contacts in a Business Advocate system.
   - **Email Queue** for email messages.
   - **Chat Queue** for text chats.

For voice, email, and chat queues, Avaya IC Manager displays the **Device Editor** that contains the same **General** tab. For details, see Specifying general device information on page 379.

For voice queues, the **Device Editor** also has a queue-specific tab called **Voice**. For details, see Specifying voice configuration options on page 382.

For Advocate Voice Parking Devices, the **Device Editor** displays the **General** tab with a unique set of Business Advocate options. For details, see Specifying Business Advocate parking device configuration options on page 383.

After you have entered the device information on these tabs, you can:

- Add the device and return to Avaya IC Manager by clicking **OK**.
- Add the new device but keep the **Device Editor** dialog open by clicking **Apply**.
- Cancel without adding the new device by clicking **Cancel**.

After adding the device, update the TSQS server if the TSQS server is already running.

- In IC Manager, right-click the TSQS server in the list of servers, and select **Update**.

Specifying general device information

You can enter the following information on the **General** tab for voice, email, and chat queues:

Id: The identifier of the device, which can be changed to eliminate confusion when multiple devices of the same type are installed. The id number may be used by more than one device for a particular media channel. Individual devices are identified by a combination of their Device ID and ACD ID.

Naming restrictions:

- The ID cannot contain any spaces.
- The ID cannot start with a 0 (zero).
- If this is a voice queue, the ID must be numeric.

If you are setting up a voice channel for:

- any switch, the ID is the VDN or vector identifier that your PBX or ACD uses for the queue.

Site: The geographic grouping that the device belongs to. In non-Business Advocate installations, this information is used by Avaya IC when it makes routing decisions. In addition, you can assign particular servers to monitor all of the queues in a specific site. For details, see Managing sites on page 37.

If you are setting up a voice channel and you want to assign a TSQueueStatistics server to monitor a voice queue, make sure that the site in the TSQS tab in the Server Editor matches both the Site and the ACD Name.

For more information about adding custom information to server records, see Changing server information.

ACD Name: The name of the associated ACD. This is only enabled for voice queues.

Name: The name or description of the device. If you are configuring a voice channel in a non-Business Advocate installation, Avaya recommends that you use the name `DefaultVoiceQueue`. If you are using Business Advocate, enter the number of the vector where the calls that are arriving at the switch reside until they are sent to a parking device or to an agent.

Naming considerations:

- The name cannot begin with (but can contain in any other position):
  - a space
  - any of the following special characters: # * @ ( ) [ ] { } - + 1 2 3 4 5 6 7 8 9 0
- If you include any leading or trailing spaces, those spaces will be removed by Avaya IC Manager when it saves the queue. You can, however, use embedded spaces, or other special characters, within the queue name.

Media: - The media type (Chat, Voice, or Email) used by the device. This field is automatically set by Avaya IC Manager based on the type of device you are creating.

Priority: The priority level assigned to the device. Set this value to 1 for the highest priority to 10 for the lowest priority.

Service Level: The period of time (in seconds) within which a queued contact should be assigned to an agent. This value is assumed to be in seconds unless it is entered in hh:mm:ss format.

Minimum Agents: The minimum number of agents assigned to the device.

Tenant: The tenant to which the device is assigned. (Tenants are not applicable to voice queues.)

Workgroup: The workgroup to which the device belongs. For more information, see Assigning devices to workgroups below. (Workgroups are not applicable to voice queues.)

Addressable: Whether the device is displayed in the Avaya Agent UAD or Avaya Agent Web Client Address Book. If selected, agents can transfer contacts to this device. This field indicates whether the virtual queue will appear in the Avaya Agent UAD or Avaya Agent Web Client Address Book.

Assigning devices to workgroups

To assign a device to a workgroup:

1. Select **Browse** in the **Workgroup** field.

   Avaya IC Manager displays the **Device Membership** dialog.
2. Select the workgroup in the **Workgroups** pane to which assign the queue will be assigned.
3. Move the workgroup into the **Member** of pane by clicking on the **Right Arrow** between the panes.

   Note:
   If you are changing the workgroup associations for a queue that is used for web routing in your production environment, you need to run the `web_routing.update_qw_cache` workflow in order to update the associations immediately. Otherwise they will not be updated until the next system refresh.
4. Select **OK** to save the device assignment and return to the **Device Editor**. The name of the tenant that the workgroup belongs to is displayed in the **Tenant** field.

Specifying voice configuration options

Avaya IC Manager displays the Voice tab if you create a voice queue. You can use this tab to specify:

Enable EDU Tracking: Determines whether Electronic Data Units (EDUs) will be tracked in a system using Multi-Site Hetero-Switch operations. When EDU Tracking is selected, the Telephony server associates individual contacts with their unique EDUID, and tracks those contacts as they navigate through the Avaya IC system. You need to select this option if you want to generate reports showing a contact's total lifecycle within the Avaya IC system. If EDU Tracking is not enabled, then the time a contact spends waiting in queue will not be recorded.

For switches that do not carry application data (used to store the EDUID of the call) across devices, if a queue is not monitored it is impossible for the TS to recognize that a call arriving at an agent from the queue is the same as the one that was routed to the queue.

Monitoring the queue ensures that the same EDUID will be tracked all the way, from the route point through the queue to the agent.

Note:
In addition to selecting this check box, make sure that the associated TS is the first one in the TS_SET list.

Wait Treatment Style: The numeric value associated with your switch's wait treatment configuration. Do not enter a value for this field.

TS Set: 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 following table gives the default size of the `voicets_set` field in different databases:

Database	Default Size
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.

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.

Specifying Business Advocate parking device configuration options

You must configure at least one parking device for each TSA server in your voice channel. However, a TSA server frequently has more than one parking device. Each parking device associated with a TSA server must use a different wait treatment style.

For details, see *IC Business Advocate Configuration and Administration*.

You can use the **General** tab to specify:

Id: The ID is the destination DN where the Telephony server sends contacts for this parking device.

Naming restrictions:

- The ID cannot contain any spaces.
- The ID must be numeric.

Site: The geographic grouping that the device belongs to. This information is used by Avaya IC when it makes routing decisions. In addition, you can assign particular servers to monitor all of the queues within a specific site. For details, see Managing sites on page 37.

ACD Name: Use the same ACD name that you configured in the Telephony server assigned to the same TSA server as the parking device.

Name: The name or description of the device.

Naming restrictions:

- The name cannot contain any spaces.
- If this queue is going to accept transfers from the Unified Agent Directory (UAD), then the name cannot exceed 32 characters in length.

Media: - The media type (Chat, Voice, or Email) used by the device. This field is automatically set by Avaya IC Manager based on the type of device you are creating.

Wait Treatment Style: What a customer hears when the customer is on hold. The wait treatment can be one or more announcements, music, or silence. The switch plays and stores the wait treatments.

You can enter any number for the wait treatment style. However, you must enter 1 if Business Advocate uses this parking device to hold transferred voice contacts.

You enter this same number in the Wait Style block of the workflow that uses this parking device.

Wait Treatment Type: Not applicable for Avaya Communication Manager.

Wait Announcement ID: Not applicable for Avaya Communication Manager.

Wait Ring Back ID: Not applicable for Avaya Communication Manager.

Announcement Length: Not applicable for Avaya Communication Manager.

TSA: The TSA server that is associated with this parking device. There should be at least one parking device per TSA with a wait treatment style of 1 for the TSA to start up and run.

You cannot assign a parking device to more than one TSA server.

Creating virtual queues

A virtual queue is a collection of voice queues, email queues, or chat that form a logical grouping as opposed to a geographical one. For example, if your company has multiple sites and each site has a voice queue, you can group all of those queues together into one virtual voice queue.

If your site uses Business Advocate, a virtual queue can also be a collection of service classes. It cannot, however, contain Business Advocate parking devices.

To create a virtual queue:

1. Select **Device > New Virtual Queue**.

   Avaya IC Manager displays the **Virtual Queue Editor**.

2. You can set the following queue options:

   - **Tenant**. The tenant to which the queue is assigned. (Tenants are not applicable to voice queues or to Business Advocate installations.)
   - **Name**. The name of the queue. This name needs to be unique across all tenants.
   - **Description**. The description of the queue.
   - **Addressable**. Whether the device is displayed in the Avaya Agent UAD or Avaya Agent Web Client Address Book. If selected, agents can transfer contacts to this device.
   - **Membership**. Select **Browse** to specify the members of this virtual queue.

To add members to the virtual queue:

1. Select **Browse** in the **Membership** field.
2. In the **Channel** field, select **Voice**, **Email** or **Chat** from the drop-down list.
3. To add a device, select **Devices**. Select the desired devices in the **Available Devices** pane and select the **Left Arrow** button to assign them to the queue.
4. To add a Business Advocate service class, select **Service Classes**. Select the desired service classes in the **Service Classes** pane and select the **Left Arrow** button to assign them to a queue. For details about service classes, see *IC Business Advocate Configuration and Administration*.

Note:
If you use Avaya Agent Web Client and you must see the latest virtual queue from the Address Book because a virtual queue has been added or deleted from Avaya IC Manager, you must refresh the Address Book from the Java Application Bridge (or reset WebConnector) and then the Agents must logout and log back into the application.

Changing device information

To change device information:

1. Select the **Device** tab on the Avaya IC Manager window.
2. Select the device or virtual queue you want to edit in the left hand pane and select **Device > Edit**.
3. Modify the information as required. (For details about the available options, see Creating devices on page 378 or Creating virtual queues on page 384.)

After you finish modifying the queue's information, you can:

- Save your changes and return to Avaya IC Manager by selecting **OK**.
- Save your changes but keep the Device Editor available by selecting **Apply**.
- Discard your changes without saving by selecting **Cancel**.

Viewing the contacts handled by each device

If you want to view the contacts that were handled by the queues in your Avaya IC system, you can use the Contact Explorer focus of the Avaya IC Report Wizard. For more information, see Displaying detailed contact information on page 200.

Deleting devices

To delete a device:

1. Select the device name in the Avaya IC Manager and select **Device > Delete**.
2. Restart any servers that are associated with the device so that they know it has been deleted.

CAUTION:
Deleting a device that is being used by a client or other process may cause an error in that process. Make sure you stop all activity to the queue, and restart the servers as soon as possible so they do not try to access the deleted device.

Chapter 17: Tables

DS Tables are loaded into the Directory server instead of being part of the application database. They can contain a variety of information, such as call routing rules, DNIS descriptions, equipment numbers and IP addresses, and announcements. They are most often used when a client application needs to display a pick-list to an agent.

You can use the tables that have been pre-defined in Avaya IC Manager, or you can create your own tables.

Note:
Before modifying tables, Avaya recommends that you backup your Directory server, as described in Backing up and restoring server configuration information on page 38.

To create or modify tables, select **Tools** > **DS Tables**. Avaya IC Manager displays the **DS Tables** dialog box that lists the current tables and the contents of the currently-selected table.

This section contains the following topics:

- Creating tables on page 388
- Deleting tables on page 389
- Entering and changing table information on page 390
- Table import and export on page 391
- Reserved table names on page 392

Creating tables

To create a table:

1. Select **Tools > DS Tables**.
2. Select **New Table** in the toolbar. Avaya IC Manager displays the **New Table** dialog box with a list of suggested table names.
3. Select the table name from the list or enter your own name in the **Table Name** field. Table names are alphanumeric, of unlimited length, case-sensitive, and may include underscores but not spaces or any punctuation marks.

Note:
The list of table names reflects how Avaya customers have used tables in the past. The data stored in a table is unrelated to the table's name (any table can be used for any purpose).

4. Select **OK** to create the table. If the table already exists or the name is reserved, Avaya IC Manager displays an error message. For a list of reserved table names, see Reserved table names on page 392.
5. To save your changes in the database, select **Commit**. If you close the **DS Tables** dialog box without committing your changes, Avaya IC Manager displays a message asking if you want to commit them. If you exit without committing the changes, Avaya IC Manager discards your changes and does not update the database.

Note:
The tables that you create using the above procedure are stored in the `ds.ffd` file and not in the database.

Deleting tables

CAUTION:
Avaya IC Manager does not validate the referential integrity of the tables. Before you delete a table, make sure that it is not being used by some other component in the Avaya IC system.

To delete a table:

1. Select **Tools > DS Tables**.
2. Select the table name in the **DS Tables** dialog box.
3. Select **Delete Table**.
4. Select **OK** at the prompt.
5. To save your changes in the database, select **Commit**.

   If you close the **DS Tables** dialog box without committing your changes, ICManager displays a message asking if you want to commit them. If you exit without committing the changes, Avaya IC Manager discards your changes and does not update the database.

Entering and changing table information

CAUTION:
Avaya IC Manager does not validate the referential integrity of the table fields. Before you change table information, make sure that the table is not being used by some other component in the Avaya IC system.

To edit an item in a table, select the item in the right pane and select Edit. In the CTI Type Editor, modify the field values as required.

Note:
You cannot change the table's Name or CTI Type. Instead, you need to delete the old item and create a new one with the correct name and type.

To add information to an existing table:

1. Select **Tools > DS Tables**. Select the table you want to modify.
2. Select **New**. Avaya IC Manager displays the **CTI Type Editor**.
3. In the **Name** field, enter the item being defined. This could be a phone extension, wrap-up code, or reason code, or, for a sequence, the name of the sequence.

   Note:
   You cannot use international characters in the item name (only in the item value).
4. In the **Values** field, enter the value for the code being defined. This could be the department associated with a phone extension or a description of a wrap-up or reason code.
5. Select **OK** to add the new item to the table. If no existing items are selected, the new field is placed at the bottom of the list. If a field is selected the new item is placed above that item. To deselect an item, click on it.
6. To add couples to a sequence, select the sequence and select **New**. In the **CTI Type Editor** dialog, select **Couple** and repeat steps 3 through 6 above.
7. To save your changes in the database, you can either enable the **Auto Commit** feature or select **Commit**. If you close the **DS Tables** dialog box without committing your changes, Avaya IC Manager displays a message asking if you want to commit them. If you exit without committing the changes, Avaya IC Manager discards your changes and does not update the database.

Tip:
To enable the Auto Commit feature, select **DS Tables** > **Auto Commit**.

Table import and export

Information can be imported into a table or exported from a table to a file. The format of the files follows the format outlined in Customizing Avaya IC Manager on page 33.

To import table information from a file:

1. Select **Tools** > **DS Tables**.
2. Select the table into which you want to import the information.
3. Select **DS Tables** > **Import**.
4. Select the file to be imported and select **OK**. The **Import Table** dialog displays a portion of the file.
5. Select the format in which this file was created and select **OK**. Table values can have commas, so you should use the "comma separated quoted" format when values have embedded commas.

   Avaya IC Manager replaces the contents of the selected table with the imported data. When it is finished, it displays a message showing the number of records that were transferred.
6. To save your changes in the database, select **Commit**. If you close the **DS Tables** dialog box without committing your changes, Avaya IC Manager displays a message asking if you want to commit them. If you exit without committing the changes, Avaya IC Manager discards your changes and does not update the database.

Exporting a table

To export a table to a file:

1. Select **Tools** > **DS Tables** and select the table that you want to export.
2. Select **DS Tables** > **Export**.
3. Specify the filename and type. Select **OK**.

   If the Auto Commit feature is not enabled and you have not saved your changes, Avaya IC Manager will prompt you to save your changes before it exports the data.

   To enable Auto Commit, select **DS Tables** > **Auto Commit**.

Reserved table names

The following table names are used by Avaya IC Manager. You can modify these tables to contain any information you like, but you cannot create a new table using the names in the right column of this table.

Description	Name
Announcements English Announcements French Canadian Announcements French Announcements Spanish	_annEnglish _annFrenchCan _annFrench _annSpanish
DNIS/Description English DNIS/Description French Canadian DNIS/Description French DNIS/Description Spanish	_dnisEnglish _dnisFrenchCan _dnisFrench _dnisSpanish
Configuration Values	_vespconfig
Media Channel Types	media_types
Reason Codes English Reason Codes French Canadian Reason Codes French Reason Codes Spanish	_reasonCodeEnglish _reasonCodeFrenchCan _reasonCodeFrench _reasonCodeSpanish
Reason Status English Reason Status French Canadian Reason Status French Reason Status Spanish	_reasonStatusEnglish _reasonStatusFrenchCan _reasonStatusFrench _reasonStatusSpanish
Reason Properties	_reasonProperties
Reason Source English Reason Source French Canadian Reason Source French Reason Source Spanish	_reasonSourceEnglish _reasonSourceFrenchCan _reasonSourceFrench _reasonSourceSpanish
Script Rules	_scriptrules
Task List	_tasklist
Equipment/IP	_tsipequipment
User Table	per

Description	Name
Server Table	srv
Scripter Table	scp
Schema Table	des

Appendix A: Database tuning and maintenance

How you tune and maintain Avaya IC and Avaya OA databases can significantly impact the performance of the Avaya IC system. This section describes some general guidelines that you should follow when you tune and maintain these databases.

Many conditions that are unique to each contact center can affect how you implement these guidelines. These conditions include contact volume, number of sites, and number of agents at each site.

This section includes the following topics:

- Consulting a qualified database administrator on page 394.
- Database tuning guidelines on page 395.
- Database maintenance on page 398.
- Creating a backup strategy on page 399.
- Creating a purging strategy on page 401.
- Related documentation on page 405.

Consulting a qualified database administrator

Before you deploy Avaya IC and Avaya OA databases or create a maintenance schedule for these databases, you should consult a qualified database administrator (DBA) or systems integrator. The DBA must possess an in-depth knowledge of database fundamentals for the installed RDBMS and operating system.

Do not use personnel who are not familiar with the RDBMS to perform database deployment or maintenance tasks.

The DBA should be involved in the following tasks:

- Determining the optimal deployment for the Avaya IC and Avaya OA databases.
- Installing and configuring the RDBMS and the databases hosted in the RDBMS.
- Monitoring the databases with RDBMS tools in a development environment and performing maintenance procedures, such as determining an optimal set-up and a maintenance procedure.
- Monitoring the databases with RDBMS tools in the production environment and performing maintenance procedures, if necessary, such as:
  - Adjust the RDBMS deployment and set-up.

- Adjust the maintenance schedule.
- Re-index the database tables.
- Defragment the database tables.
- Devise an optimal data placement strategy that can include:
  - Locate database tables in different disks.
  - Split table spaces across different disks.
  - Store data on different disks than the operating system and RDBMS software to minimize I/O contention.

Database tuning guidelines

Database tuning should be one of the regularly scheduled maintenance tasks for Avaya IC and Avaya OA databases. After you complete the initial deployment and configuration of the databases, a qualified DBA should monitor the performance of the database and adjust the tuning and deployment, if necessary.

This section describes some of the issues that can require updates to the database tuning and some suggestions of how to handle these issues. This section includes the following topics:

- Database table growth rates on page 395.
- Database queries on page 397.
- Transaction logs on page 397.

Tip:
The documentation provided with the RDBMS includes tuning suggestions. Consult a qualified DBA and that documentation for additional tuning guidelines and information on how to implement the recommended tuning strategies.

Database table growth rates

The configuration of an Avaya IC system impacts the growth rate of the database tables. This section identifies some tables that you need to watch. However, a qualified DBA should monitor the growth of all tables in Avaya IC and Avaya OA databases, especially tables in IC Repository.

This section includes the following topics:

- Consequences of table growth on page 396.
- Strategies for table growth on page 396.
- Tables to watch in IC Repository on page 396.

- Tables to watch with Email Management on page 396.

Consequences of table growth

If database tables grow too large, updates to existing data can cause fragmentation of the data in the tables, row migration, and row chaining. These consequences can seriously impact the performance of an Avaya IC system.

Strategies for table growth

If some database tables have grown so large that they have impacted performance, you can do one of the following:

- Partition tables.
- Locate the database tables with a high rate of growth across multiple disks on the database machine.
- Include defragmentation of the database in the regular maintenance schedule.
- Re-index the tables.
- Update table statistics.

Tables to watch in IC Repository

For all Avaya IC systems, the following database tables in IC Repository will grow in conjunction with the number of transactions:

- contact
- routingevent
- mediainteraction

Tables to watch with Email Management

For Avaya IC systems with Email Management, the following database tables in the CallCenterQ database will grow in parallel:

- qem_message
- qem_messagestatlog

Database queries

Most components of Avaya IC perform database queries through the Data server. The configuration of an Avaya IC system and the workflows in that system impact the frequency of database queries.

This section identifies some queries that you need to watch. However, a qualified DBA should monitor the frequency of queries against the Avaya IC database. This section includes the following topics:

- Strategies for frequent database queries on page 397.
- Queries to watch on page 397.

Strategies for frequent database queries

To enhance the performance of an Avaya IC system, make sure that all frequently run stored procedures are pinned to the cache. When you pin a stored procedure to the cache, that procedure does not age out of memory.

Queries to watch

For all Avaya IC systems, the following database queries occur frequently during normal operation:

- Queries for customer record data
- Queries for agent login data

Transaction logs

The transaction log captures changes to data, such as additions, deletions, and updates. You can use the transaction log to assist with the backup recovery of an Avaya IC database.

This section describes the recommended mode for transaction logs, and some strategies you can implement to take maximum advantage of transaction log capabilities. This section includes the following topics:

- Recommended transaction log mode on page 397.
- Strategies for transaction logs on page 398.

Recommended transaction log mode

Avaya recommends that you configure transaction logs in the following modes:

- For DB2, use log retain mode.
- For Oracle, use archive log mode.
- For SQL Server use transaction log mode.

Strategies for transaction logs

To avoid serious impact to the performance of an Avaya IC system, monitor the size of the transaction logs and do the following, if necessary:

- Create the transaction log on a physically separate disk or RAID (redundant array of independent disks) device.
- Adjust the size of the transaction log file to prevent the file from expanding too frequently.
- Adjust the growth increment percentage to prevent the file from growing by too small a value.

Database maintenance

In addition to periodic tuning, a qualified DBA should regularly monitor and perform maintenance on the Avaya IC and Avaya OA databases.

This section includes the following topics:

- Scheduling maintenance procedures on page 398.
- Using database tools to check performance on page 398.

Scheduling maintenance procedures

Certain maintenance procedures, such as backups and re-indexing, can impact database performance. Consider the following guidelines when you schedule maintenance procedures:

- If possible, schedule all backups during non-business hours.
- For a 24-by-7 contact center, review the contact load reports and schedule all backups to run during low traffic periods.
- For Avaya OA databases, do not schedule a backup to run at the same time as system-scheduled jobs, such as Purge or Aggregation recovery.

Using database tools to check performance

Each supported RDBMS includes a set of database tools that a qualified DBA can use to monitor the performance of the database and determine when the database needs to be tuned.

Frequency of performance checks

Include a performance check with the database tools in your regular database maintenance schedule. Avaya recommends that you perform this check at least once per week.

Reacting to changes in performance metrics

As data is added to the database, performance metrics will change. For example, as database tables grow, database queries can take longer to complete. When the database tools show that the metrics have changed, a qualified DBA should tune the database.

For guidelines on how to tune the database, see Database tuning guidelines on page 395 and the documentation provided with the RDBMS.

Creating a backup strategy

This section describes the general guidelines for a database backup strategy. This section includes the following topics:

- Backup responsibilities on page 399.
- Types of backups on page 400.
- Minimum frequency of backups on page 400.
- Recommended backup strategies on page 400.

Backup responsibilities

A trained DBA or other qualified person should customize and perform all of your backup operations. As part of their backup responsibilities, the DBA should:

- Define the types of backups required.
- Schedule regular backups.
- Manage tape backups to ensure that the tapes for all databases are backed up and labelled correctly.

Types of backups

Avaya recommends that your backup strategy include a combination of incremental backups and full backups.

A full backup captures a snapshot of a database at a point in time. This backup provides a copy of the entire database from which the databases could be restored in the event that the database is lost or corrupted.

An incremental backup captures only the changes that have occurred in the data since the last backup, either full or incremental. To restore from incremental backups requires a full backup and all incremental backups since the full backup.

Minimum frequency of backups

Schedule regular backups of all Avaya IC and Avaya OA databases. Avaya recommends the following as a minimum backup frequency:

- Perform a full backup once a week.
- Perform an incremental backup once each day.

Recommended backup strategies

The contact load and database activity of a contact center determines the best backup strategy for a contact center. These factors can change over time. Periodically review the Avaya OA reports on contact load and agent activity, and the results of the performance checks to determine if you need to adjust your backup strategy to better protect your data from loss.

The following table summarizes the backup strategies recommended by Avaya.

Contact load	Backup strategy
Small	• Full backup of all databases daily • Transaction log backups every 30 minutes for Microsoft SQL Server and IBM DB2 • Archive log backups every 30 minutes for Oracle

Contact load	Backup strategy
Medium	• Full backup of all databases weekly • Incremental backups daily • Transaction log backups every 30 minutes for Microsoft SQL Server and IBM DB2 • Archive log backups every 30 minutes for Oracle
Large	• Full backup of all databases weekly • Incremental backups daily • Transaction log backups every 30 minutes for Microsoft SQL Server and IBM DB2 • Archive log backups every 30 minutes for Oracle

Creating a purging strategy

This section describes general considerations and guidelines for a strategy to purge and archive data in database tables. These guidelines apply to all supported RDBMS.

This section includes the following topics:

- Considerations for a purging strategy on page 401.
- Recommended criteria for purging strategy on page 402.
- Relationships between database tables on page 403.
- Historical contact data on page 404.
- Email contact data on page 404.
- Chat contact data on page 405.

Considerations for a purging strategy

When you create a purging strategy, consider the following:

- Relationships between the tables in an Avaya IC database
- Relationships between the tables across more than one Avaya IC database
- Criteria that will drive the purging strategy

Important:
If the Avaya IC system includes a customized database schema, you must consider those customizations and any new table relationships when you create a purging strategy.

Recommended criteria for purging strategy

Avaya recommends that you use the `createtime` field in the Contact table of IC Repository as the main criteria to drive your purging strategy.

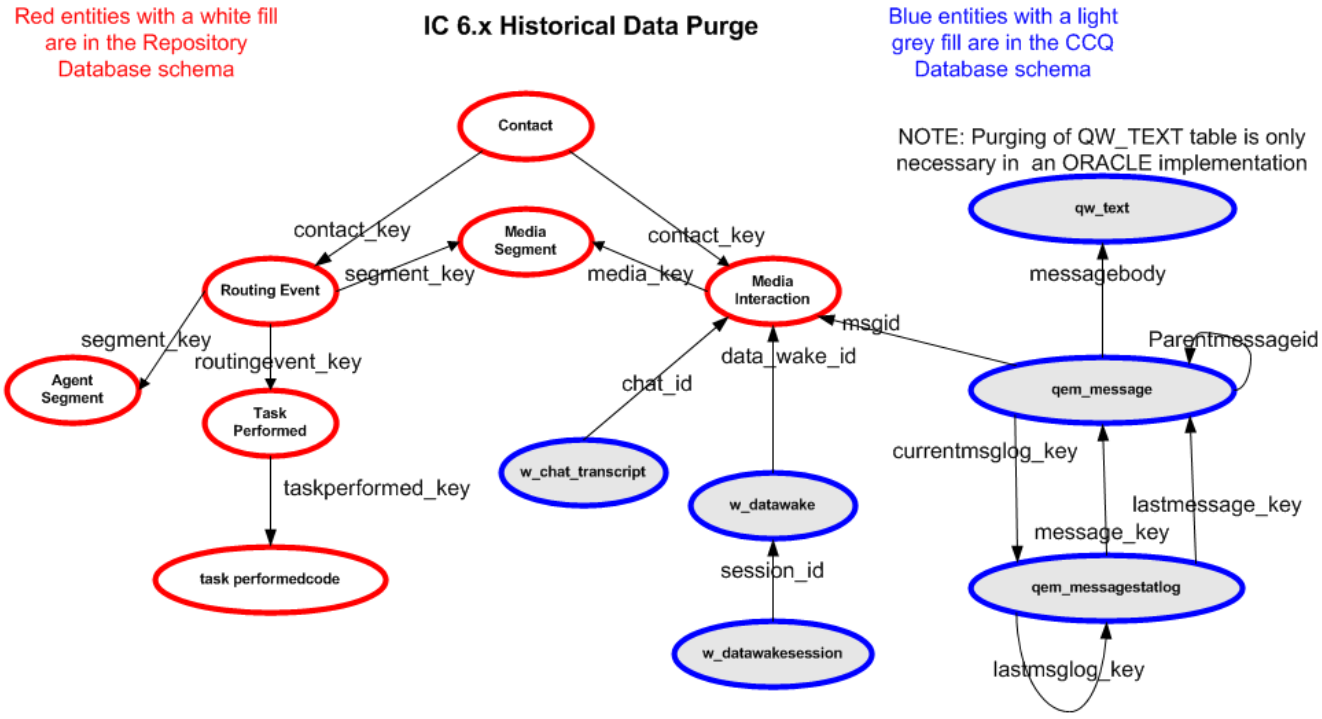
Running optimization procedures

Avaya recommends running optimization procedures to reindex the tables on the database, to improve performance of queries and other sql operations. However, the optimization procedure will impact the performance of IC. For example, indexing of contact or mediainteraction tables may lock the respective indexes for those tables. In that case, INSERTs into those tables will fail, causing ROLLBACKs on the transaction logs. Optimizating should be run during maintenance windows when IC is down, or in the case of 24x7 sites, at the least busy times.

Purging is recommended to streamline the historical tables on the database. However, the DELETE operation, particularly when large numbers of rows are being deleted, may tend to lock the indexes on the tables as well. This implies the same problem as the optimization process for the ReportServer INSERTs, which will cause ROLLBACKs. The purge process should be run during maintenance windows when IC is down, or in the case of 24x7 sites, at the least busy times.

Relationships between database tables

Before you create a purging strategy, you must review and consider the relationships between the database tables. The following diagram identifies some tables in IC Repository and the CallCenterQ database, and the relationships between these tables.



Relationships identify the foreign field in the child table that points back to the primary key in the parent table. Note: There is database enforced referential integrity between all tables in the same schema, there is no referential integrity check across database schemas

Historical contact data

Historical contact data is the data that relates to the processing of a contact. Historical contact data is keyed off the Contact table in IC Repository.

To create a purging strategy that focusses on historical contact data, use the `createtime` field in the Contact table. The `createtime` field contains the date and time that a contact was first processed by Avaya IC. The data in this field works well as the main criteria for purging.

Avaya recommends that you use the `createtime` field in the Contact table as the main criteria for your purging strategy.

Email contact data

Email contact data includes data about each email contact and a history that links related emails. Email contact data is keyed off the tables in the CallCenterQ database. The following table describes those tables.

Database table	Description
qem_message	The primary table that holds data about each email contact, including the date and time that the email contact was first processed and the body of the email message.
qem_messagestatlog	A secondary table that holds a duplicate history which is used internally to link related email contacts.
qw_text	For Oracle databases only. A table that holds the blob data in the `messagebody` field of the qem_message table. The `messagebody` field in qem_message contains an integer for the key to the record in the qw_text table that contains the actual text blob.

The CallCenterQ database includes circular relationships between the qem_message table and the qem_messagestatlog table. These relationships require you to clear some of the values from the foreign field.

If your Avaya IC system includes Email Management, and you choose not to use the Contact table in IC Repository, you can use the `createtime` field in the qem_message table. However, Avaya does not recommend this approach.

Chat contact data

Chat contact data can include the DataWake history and the transcripts of chat contacts, depending upon whether the Avaya IC system includes these features. Each group of chat contact data is distinct. The data for these features is in the following database tables:

DataWake history: The w_datawakesession table in the CallCenterQ database contains the DataWake history. You can use the `dt_begin` field in the w_datawakesession table as the criteria for purging. However, Avaya does not recommend this approach.

Chat transcripts: The mediainteraction table in IC Repository contains the information about the chat transcripts. This table does not include a field that identifies the date of each transcript. You must identify the transcripts from the selection of records available to be purged from the mediainteraction table. You do not need to purge any related tables in the Avaya IC databases when you purge chat transcripts.

You can purge chat transcript data separately. However, Avaya does not recommend this approach.

Related documentation

Consult the following documentation when you create a deployment and maintenance strategy for Avaya IC and Avaya OA databases:

- *IC Installation Planning and Prerequisites*
- *OA Maintenance and Troubleshooting*
- Documentation provided by the manufacturer of the RDBMS

Appendix B: Database Purge

Avaya Interaction Center (IC) 7.2 changed the Email Server design, due to which emails are stored in database in chunks. There are multiple tables where information related to same email gets stored. From contact history point of view, all emails that are part of same email interaction and have the same tracking number are needed.

This chapter contains guidelines for purging emails from the IC database so as to avoid partial purging of email interactions. Partial purging of emails from the database might lead to a database search failure for contact history.

Note:
You must ensure to take a backup of the database before performing database purge.

Database purge of IC Repository and CallCenterQ database tables for MSSQL 2008, 2010, and 2014

Guidelines for purging of emails from IC Repository and CallCenterQ database tables

- The purging procedure must be carried out by a Database Administrator.
- IC must be shut down before starting the Purge tool. The Purge tool does not verify whether IC is running.
- The purging date range criterion does not consider Daylight Savings Time (DST).
- There is no suitable benchmarking done for the performance of running the scripts.
- Avaya recommends that the Database Administrator backs up the repository and CallCenterQ (CCQ) databases before carrying out the purge operation.
- Avaya recommends that the Database Administrator tests the procedures on a lab system and then re-runs the procedures on a production system.
- MS SQL Server Management studio must be available for running the purge procedures.

Overview of the purging process

1. Following table data is purged for email, chat, and voice contacts of the IC repository database:
   - Contact
   - MediaInteraction
   - MediaSegment
   - Routingevent
   - AgentSegment
   - TaskPerformed
   - TaskPerformedCode
   - routingattempt
   - menupresentation
   - mktngannouncement
2. The stored procedure can preview the number of rows in the Contact table in the repository database that would get deleted. The Contact table is the primary table on which the purging decision is taken. The rest of the tables are considered to be dependent tables of the Contact table.
3. Following tables are targeted for purging of email data from the IC CCQ database:
   - qem_message
   - qem_messagechunks
   - qem_messagestatlog
   - qw_qualifier
4. Following tables are targeted for purging of chat data from the IC CCQ database:
   - w_chat_transcript
   - w_chat_wrap_survey
   - w_datawake
   - w_datawakesession
   - w_task_type_sum
   - w_task_detail
5. The stored procedure also deletes the rows of the dependent tables.
6. The stored procedure accepts the following three parameters:
   a. Start date for entry search.
      For example, if 2015-02-01 is specified as the 1st parameter, then the stored procedure retains data starting from February 1st of 2015.

b. End date for entry search.
For example, if 2016-03-01 is specified as the 1st parameter, then the stored procedure retains data starting from March 1st of 2016.

c. The third parameter accepts the following values:

1. @PrintRows : 1: Prints the number of rows from the Contact table of the IC Repository that are targeted for deletion. This is default value, if the argument is not specified.
2. @PrintRows: 0: Disables the preview mode and indicates actual execution of the purge scripts.

7. If the purge operation is successful, the data is committed to the database.
8. If the purge operation is unsuccessful, the data is rolled back.
9. The number of records of the main table that are targeted for purge is based on following SQL function derivation:

```
createtime between @startDate and @endDate
```

Where,
createtime = Record create time
startDate= Start date for entry search
endDate= End date for entry search
The SQL function derivation example is for the Contact table in the IC Repository.
A similar formula is used for the CCQ database for calculating number of records to be deleted from the anchor table.

Purging of data from the IC Repository and the CallCenterQ database tables - High level steps

1. Copy the following scripts to the IC database client or server machine:
   a. `msContactHistory.proc.sql` for the IC Repository database
   b. `msspDeleteRows.proc.sql` for the IC Repository database
   c. `msChatTables.proc.sql` for the CallCenterQ (CCQ) database
   d. `msEmailTables.proc.sql` for the CCQ database
2. Include the stored procedure scripts mentioned previously as part of the Repository or CCQ database and prepare to run the scripts.
3. Run the stored procedure scripts to purge data from the Repository or CCQ database.

Purging of data from the IC Repository database tables

1. Copy the scripts on to the local drive of the IC database client or server from where you can run scripts using SQL Management studio.
2. Open SQL Management studio and connect to the instance having the IC repository database.
3. Open the `msspDeleteRows.proc.sql` file in SQL Management studio using **File > Open > File**.
4. Change the repository database name and database schema name appropriately, if the names are different from those mentioned.
5. To test the syntax, click **Query > Parse**.
6. To create the stored procedure, click **Query > Execute**.
7. Follow steps 1 to 6 for the `msContactHistory.proc.sql` stored procedure.
8. Ensure that you grant suitable execute permissions to the stored procedure scripts. The permission granted must be Database Role > public.
   For more information see, http://technet.microsoft.com/en-us/library/ms345484.aspx.
9. In the object explorer, click **Repository database > Programmability > Stored Procedures** and ensure that the following two stored procedures, prefixed by their schema names are listed:
   - purgecontacthistorytables
   - spDeleteRows

   Important:
   You are required to perform steps 1 to 9 only once.
10. Right click the purgecontacthistorytables stored procedure and then click the **Execute Stored Procedure …** menu item.
11. Type the argument values for the following parameters:
    a. @startDate
       You must type the startDate in the YYYY-MM-DD format.
    b. @endDate
       You must type the endDate in the YYYY-MM-DD format.
    c. PrintRows
12. (Optional) To view the messages displayed by the script, click the **Messages** tab.
13. Perform the same steps for executing the spDeleteRows stored procedure.

Purging of data from the CallCenterQ database tables

1. Copy the scripts on to the local drive of the IC database client or server from where you can run scripts using SQL Management studio.
2. Open SQL Management studio and connect to the instance having the IC repository database.
3. Open the `msEmailTables.proc.sql` file in SQL Management studio using **File > Open > File**.
4. Change the CCQ database name and database schema name appropriately, if the names are different from those mentioned.
5. To test the syntax, click **Query > Parse**.
6. To create the stored procedure, click **Query > Execute**.
7. Follow steps 1 to 6 for the `msChatTables.proc.sql` stored procedure.
8. Ensure that you grant suitable execute permissions to the stored procedure scripts. The permission granted must be Database Role > public.
   For more information see, http://technet.microsoft.com/en-us/library/ms345484.aspx.
9. In the object explorer, click **Repository database > Programmability > Stored Procedures** and ensure that the following two stored procedures, prefixed by their schema names are listed:
   - purgechattables
   - purgeemailtables

   Important:
   You are required to perform steps 1 to 9 only once.
10. Right click the purgechattables stored procedure and then click the **Execute Stored Procedure …** menu item.
11. Type the argument values for the following parameters:
    a. @startDate
       You must type the startDate in the YYYY-MM-DD format.
    b. @endDate
       You must type the endDate in the YYYY-MM-DD format.
    c. PrintRows
12. (Optional) To view the messages displayed by the script, click the **Messages** tab.
13. Perform the same steps for executing the purgeemailtables stored procedure.

Database purge of IC Repository and CallCenterQ database tables for Oracle 10g and Oracle 11.x g

Guidelines for Purging of emails from IC Repository and CallCenterQ database tables

- The purging procedure must be carried out by a Database Administrator.
- IC must be shut down before starting the Purge tool. The Purge tool does not verify whether IC is running.
- The purging date range criterion does not consider Daylight Savings Time (DST).
- There is no suitable benchmarking done for the performance of running the scripts.
- Avaya recommends that the Database Administrator backs up the repository and CCQ databases before carrying out the purge operation.
- Avaya recommends that the Database Administrator tests the procedures on a lab system and then re-runs the procedures on a production system.
- Oracle SQL Developer application must be available for running the purge procedures.

Overview of the purging process

1. Following table data is purged for email, chat, and voice contacts of the IC repository database:
   - Contact
   - MediaInteraction
   - MediaSegment
   - Routingevent
   - AgentSegment
   - TaskPerformed
   - TaskPerformedCode
   - routingattempt
   - menupresentation
   - mktngannouncement

2. The stored procedure can preview the number of rows in the Contact table in the repository database that would get deleted. The Contact table is the primary table on which the purging decision is taken. The rest of the tables are considered to be dependent tables of the Contact table.
3. Following tables are targeted for purging of email data from the IC CCQ database:
   - qem_message
   - qem_messagechunks
   - qem_messagestatlog
   - qw_text
   - qw_qualifier
4. Following tables are targeted for purging of chat data from the IC CCQ database:
   - w_chat_transcript
   - w_chat_wrap_survey
   - qw_text
   - w_datawake
   - w_datawakesession
   - w_task_type_sum
   - w_task_detail
5. The following tables are created to list the purge ids:
   - For email
     - qem_message_pkeyset
     - qem_messagestatlog_pkeyset
   - For chat
     - w_datawakesession_idset

Note:
The stored procedures create a few temporary tables during the purge operation. Therefore, you must ensure that there is scope for creating enough table space on the database server machine. After the purge operation is completed these pkeys are removed.

6. The COMPLETEDEMAILTHREADS view is created for email purge operation. The COMPLETEDEMAILTHREADS view lists the completed email threads.
7. The stored procedure also deletes the rows of the dependent tables.
   a. Start date for entry search.
      For example, if 01-02-2015 is specified as the 1st parameter, then the stored procedure retains data starting from February 1st of 2015.

b. End date for entry search.
For example, if 01-03-2016 is specified as the 1st parameter, then the stored procedure retains data starting from March 1st of 2016.

c. The third parameter accepts the following values:

1. @PrintRows : 1: Prints the number of rows from the Contact table of the IC Repository that are targeted for deletion. This is default value, if the argument is not specified.
2. @PrintRows: 0: Disables the preview mode and indicates actual execution of the purge scripts.

8. If the purge operation is successful, the data is committed to the database.
9. If the purge operation is unsuccessful, the data is rolled back.
10. The number of records of the main table that are targeted for purge is based on following SQL function derivation:

`createtime between STARTDATE and ENDDATE`

Where,
createtime = Record create time
STARTDATE= Start date for entry search
ENDDATE= End date for entry search
The SQL function derivation example is for the Contacts table in the IC Repository.
A similar formula is used for the CCQ database for calculating number of records to be deleted from the anchor table.

Purging of data from the IC Repository and the CallCenterQ database tables - High level steps

1. Copy the following scripts to the IC database client or server machine:
   a. `oraContactHistory.proc.sql` for the IC Repository database
   b. `oraContact.proc.sql` for the IC Repository database
   c. `oraChatTables.proc.sql` for the CallCenterQ (CCQ) database
   d. `oraEmailTables.proc.sql` for the CCQ database
2. Include the stored procedure scripts mentioned previously as part of the Repository or CCQ database and prepare to run the scripts.
3. Run the stored procedure scripts to purge data from the Repository or CCQ database.

Purging of data from the IC Repository database tables

1. Open `oraContactHistory.proc.sql` in a suitable editor and search and replace all the string occurrence of <schema> with the Repository schema name and then save and close the file.
2. Open `oraContact.proc.sql` in a suitable editor and search and replace all the string occurrence of <schema> with the Repository schema name and then save and close the file.
3. Connect to the IC repository database using either database administrator or repository schema user credentials.
4. In Oracle SQL Developer, click **Open** to open the `oraContactHistory.proc.sql` file.
5. Ensure that you select the appropriate database before you compile the script in case the user has permissions for multiple databases.
6. To execute the script, press **F5** or run the **`Run script`** command.
   If you do not encounter any issues while running the script, then the system creates the DELETECONTACTHISTORY stored procedure.
7. Repeat steps 4 to 6 for the `oraContact.proc.sql` script.
   If you do not encounter any issues while running the script, then the system creates the PURGECONTACTTABLES stored procedure.
8. Grant suitable execute permissions to the stored procedure scripts by right clicking the stored procedure and then clicking **Grant**.
   Select appropriate user and EXECUTE privileges.

   Important:
   You are required to perform steps 1 to 8 only once.
9. Right click the PURGECONTACTTABLES stored procedure and then click the **Run** menu item.
10. Type the argument values for the following parameters:
    a. STARTDATE
       You must type the STARTDATE depending on the values set in the **Date Language** and **Date Format** fields in your Oracle SQL Developer client.

Note:
Check the values set in the **Date Language** and **Date Format** fields in the SQL Developer client using the following steps:

1. In the SQL Developer client menu, click **Tools > Preferences**.
2. In the Preferences dialog box, from the left pane, click **Database > NLS Parameters**.

3. Verify the values set in the **Date Language** and **Date Format** fields.

   You must use the same date format in the purge scripts that is present in the **NLS Parameters.**
   For example if the Date Language is set to English and the Date Format is DD.MM.YYYY, which can be displayed as DD.MM.RR on the NLS Parameters page, then you must type the STARTDATE as 21.02.2016. However if the Date Language is set to English and the Date format is DD.MON.YYYY, then you must type the STARTDATE as 21.FEB.2016.

b. ENDDATE
   You must type the ENDDATE depending on the values set in the **Date Language** and **Date Format** fields in your Oracle SQL Developer client.
   You must check the values set in the **Date Language** and **Date Format** fields in the SQL Developer client using the steps mentioned in STARTDATE step.

c. PRINTROWS

11. Check the output log messages after you have run the stored procedure.

Purging of data from the CallCenterQ database tables

1. Open `oraChatTables.proc.sql` in a suitable editor and search and replace all the string occurrence of <schema> with the CCQ schema name and then save and close the file.
2. Open `oraEmailTables.proc.sql` in a suitable editor and search and replace all the string occurrence of <schema> with the CCQ schema name and then save and close the file.
3. Connect to the IC database using either database administrator or CCQ schema user credentials.
4. In Oracle SQL Developer, click **Open** to open the `oraChatTables.proc.sql` file.
5. Ensure that you select the appropriate database before you compile the script in case the user has permissions for multiple databases.
6. To execute the script, press **F5** or run the **`Run script`** command.
   If you do not encounter any issues while running the script, then the system creates the PURGECHATTABLES stored procedure.
7. Repeat steps 4 to 6 for the `oraEmailTables.proc.sql` script.
   If you do not encounter any issues while running the script, then the system creates the PURGEEMAILTABLES stored procedure.
8. Grant suitable execute permissions to the stored procedure scripts by right clicking the stored procedure and then clicking **Grant**.
   Select appropriate user and EXECUTE privileges.

   Important:
   You are required to perform steps 1 to 8 only once.

9. Right click the PURGECHATTABLES stored procedure and then click the **Run** menu item.

10. Type the argument values for the following parameters:
    a. STARTDATE
       You must type the STARTDATE depending on the values set in the **Date Language** and **Date Format** fields in your Oracle SQL Developer client.
       You must check the values set in the **Date Language** and **Date Format** fields in the SQL Developer client using the steps mentioned in the Purging of data from the IC Repository database tables topic.
    b. ENDDATE
       You must type the ENDDATE depending on the values set in the **Date Language** and **Date Format** fields in your Oracle SQL Developer client.
       You must check the values set in the **Date Language** and **Date Format** fields in the SQL Developer client using the steps mentioned in the Purging of data from the IC Repository database tables topic.
    c. PRINTROWS
11. Check the output log messages after you have run the stored procedure.
12. Right click the PURGEEMAILTABLES stored procedure and then click the **Run** menu item.
13. Type the argument values for the following parameters:
    a. STARTDATE
       You must type the STARTDATE depending on the values set in the **Date Language** and **Date Format** fields in your Oracle SQL Developer client.
       You must check the values set in the **Date Language** and **Date Format** fields in the SQL Developer client using the steps mentioned in the Purging of data from the IC Repository database tables topic.
    b. ENDDATE
       You must type the ENDDATE depending on the values set in the **Date Language** and **Date Format** fields in your Oracle SQL Developer client.
       You must check the values set in the **Date Language** and **Date Format** fields in the SQL Developer client using the steps mentioned in the Purging of data from the IC Repository database tables topic.
    c. PRINTROWS
14. Check the output log messages after you have run the stored procedure.

Appendix C: Server configuration reference

This section describes the server specific configuration parameters for all of the standard Avaya IC servers.

CAUTION:
Use caution when modifying server configuration parameters because errors can seriously impact your Avaya IC system. You should set your security privileges accordingly.

If you modify configuration parameters for a server, you must stop and restart the server for the new settings to take effect. Starting and stopping servers must be done carefully because it can impact the regular operation of Avaya IC or result in data loss. This becomes even more critical when you need to stop multiple servers due to dependencies between the servers. Before starting and stopping servers on Avaya IC, see Determining server start up or shutdown dependencies on page 75 for more detailed information.

This section contains the following topics:

- ADU (Agent Data Unit) server on page 420
- Alarm server on page 428
- Attribute server on page 432
- Blender server on page 434
- CAAdmin (Content Analyzer Administration) server on page 438
- CA (Content Analyzer) server on page 440
- ComHub server on page 443
- Data server on page 445
- Directory server on page 453
- DUStore server on page 458
- EAI server on page 460
- EAI Email server on page 460
- EAI Workflow server on page 460
- EDU (Electronic Data Unit) server on page 460
- Event Collector server on page 469
- Event Collector Bridge server on page 472
- HTTP Connector server on page 473
- HTTPVOX server on page 477

- Email server on page 482
- Log Collector server on page 485
- Java Application Bridge server on page 488
- License server on page 493
- Notification server on page 496
- ORB server on page 500
- Paging server on page 502
- Poller server on page 504
- Report server on page 510
- Resource Manager server on page 513
- SiebelAED server on page 515
- SiebelAICD server on page 515
- SiebelASIS server on page 515
- TS (Telephony) servers on page 515
- Telephony Queue Statistic servers on page 526
- TSA (Telephony Services Adaptor) server on page 528
- VOX server on page 531
- WAA (Web Advocate Adaptor) server on page 540
- WebACD server on page 542
- Web Scheduled Callback server on page 550
- WebServices server on page 553
- Workflow server on page 556
- Recommended server parameter settings on page 564

Before configuring servers

Read this section before you configure the servers described in this chapter.

The following characters are reserved because they have special meaning in Avaya IC. These characters cannot be present in the values of any server configuration. When entering text in the server configuration fields, do not use these reserved characters.

Character	Description
(	Left parentheses
)	Right parentheses
[	Left bracket
]	Right bracket
{	Left brace
}	Right brace
,	Comma
\	Backslash
"	Quotation mark

ADU (Agent Data Unit) server

The Agent Data Unit (ADU) server is responsible for tracking the state of agents at the contact center. When an agent logs into Avaya Interaction Center (Avaya IC), the ADU server creates an Agent Data Unit, which is a record of the agent's session on Avaya IC. ADUs are also used to represent queues and other entities. The ADU server manages the ADU throughout its lifecycle. It creates new ADUs, stores open ADUs, and provides services for clients to interact with an agent's record. When an agent ends a session on Avaya IC, the ADU server terminates that agent’s ADU.

For details, refer to *Agent Data Unit Server Programmer Guide*.

This section contains the following:

- General tab on page 421
- ADU tab on page 421
- Persistence tab on page 426
- Configuration tab on page 427
- Debug tab on page 428
- Advanced tab on page 428

General tab

Field	Recommended entry	Notes
Name	ADU_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya 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, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

ADU tab

Field	Recommended entry	Notes
Idle Time (min)	Enter the number of minutes an ADU may remain inactive before being terminated. Default is 90 minutes. Minimum is 1 minute, maximum is 12 hours.	Inactive means that none of the clients interested in this ADU has read or written anything to the ADU in this period of time. Make sure that the number of minutes entered in this field is greater than the length of a typical agent's shift. For example, if an agent in your contact center typically works a nine hour shift (including lunch), enter 540 in this field. When the ADU is terminated because of idle time, the agent is logged out.
No User Interval (sec)	Enter the minimum number of seconds an ADU may reside in memory after all of the clients have terminated their interest in it. Default is 60 seconds. Minimum is 1 second, maximum is 60 minutes.	Very low values may cause thrashing if cooperating applications allow any gap passing ADUs among themselves.

Field	Recommended entry	Notes
Random Kill Interval (sec)	Enter the maximum number of seconds an ADU stays in memory after the usual timers have expired. Default is 30, the range is 1 to 120 seconds.	Random intervals are useful when a large number of ADUs are simultaneously terminated causing the IC Repository and the DUStore server to be flooded with requests. Handling the requests over a 2-minute period decreases database server stress. In situations where this is unlikely, more predictable timing and better memory usage result from a setting of 1. While testing to see if ADUs are being retired when they should be, 1 is also an appropriate setting.
Scan Interval (sec)	Enter the number of seconds to wait between checking various ADU server timers. Default is 4 seconds. Minimum is 1 second, maximum is 60 seconds.	Higher values may save some CPU time; lower values make for more predictable behavior during prototyping and testing. Assume that other timers in the ADU could be off by as much as (this interval + 1) to start.
Max Active ADUs	Enter the maximum number of ADUs that the ADU server keeps active at the same time. Default is 4,096	If more than this number of ADUs are created, the ADU server sends an alarm and forcibly terminates the oldest one to make room for each new one. This value should be somewhat greater than the number of agents and VRU lines using this server to handle calls. The default varies by release. Always set this value explicitly.
Allowed Assigns	Enter the number of clients interested in assigning to ADU servers. Default is 8,192	To start, this should be equal to the number of agents in the contact center (or across all contact centers in a WAN environment), plus a few extra.
Suspend Interval (sec)	Enter the number of seconds before an ADU, which is suspended by use of the Suspend method by all users, is considered for Suspension. Default is 5 seconds. Minimum is 1 second. Maximum is 1200 seconds (20 minutes).	This parameter can be overridden by a higher value in the Suspend method.

Field	Recommended entry	Notes
Advanced Properties		
Enable Reporting Interface	Check to enable reporting. Default is checked.	Checking this field displays the "filter" parameter, which is described at the end of this table.
Pool Size	Enter the initial amount of memory allocated for data belonging to each ADU. Default is 2000.	Increase the pool size if a large amount of data is stored and performance needs to be improved.
Pool Growth Increment	Enter the amount of memory (in mg) by which to increase pool size allocation when more memory is needed to store strings or events. Default is 1024.	
Initial Number of Fields	Enter the number of fields expected in an ADU. Default is 128. If using containers, increase this value to 256 or 512.	This parameter does not limit the number of fields, but when this number is exceeded, the server must reallocate space.
Pool Re-Pack (%)	Specify the percentage of memory that is free in the ADU pool, when the ADU server will repack the pool to save memory. Default is 25.	Sites at which performance is critical and memory is plentiful should consider using a value of 100.
Poll Wait (ms)	Enter the interval value, in hundredths of a second, for the IC Toolkit's Select() method. Default value is 2 (20 milliseconds).	Low values increase CPU utilization. High values (over 100) may affect the accuracy of the scaninterval parameter.
Maximum Number of Revisions	Enter the number of revisions of a value kept for access with the GetValuesHistory() method. Default is 1, which is generally recommended.	Caution: Do not enter 0 in this field. If this 0 is entered, the ADU server keeps all revisions, which could result in a failure due to lack of system resources.
Maximum Number of Cached ADU events	Enter the maximum number of events to be kept in memory for each ADU. Default is 256.	A setting of 64 is recommended as a reasonable number of events to be kept in memory. High values may increase Eventsink throughput. Low values may conserve memory.

Field	Recommended entry	Notes
Subcontainer Instances	Enter the number of instances of a subcontainer created with the + token that can exist at one time, in the format <containername>.<integer>. If more instances than this number are created, the earliest instance is deleted. Default is 0, which specifies no limit (all instances of a subcontainer are kept). A setting of 4 is recommended.	The containers that must be configured with instance limits are chat, email, voice, and ts.
Retry Interval (sec)	Enter the number of seconds to wait between automatic attempts to reassign to IC servers. Default is 60 (1 minute) Minimum is 6 seconds Maximum is 172800 seconds (48 hours)	It is not recommended to set this value below 30 seconds in a production environment. It performs a synchronous DS call for a list of ADU servers and attempts an asynchronous Assign to any of them that it isn't already assigned to. If the Assign fails (the request function itself fails), the offending ADU server is removed from the list and not retried automatically. The retry is only attempted if the Assign callback reveals an error or a ServerFailed event arrives.
Reset Interval	Enter the number of seconds to wait between attempts to reassign to servers after receiving an ADU.FailADUCon alarm. Default is 2 seconds. Minimum is 0 Maximum is 172800 seconds (48 hours)	
Data Element Names	Enter the names of the data elements in ADU events to be sent to the server specified on the Event Sink option.	Enter each element on the Edit dialog. If this option is not set, all data elements are stored. The ADUID field is always stored. The use of wildcards is permitted. Use this parameter with care; filtering elements from the End event may adversely affect reporting capability.

Field	Recommended entry	Notes
ADU Data Percent	Enter the percentage of ADUs that are sent to the ADU data feed, to be used for random sampling. Default is 0 Minimum is 0 Maximum is 100	Setting this field to anything other than 0 results in Alarms. Other settings of this feature are designed for future functionality.
Filter	Set the filter to determine which ADU events are sent to the Report server. Event types are start, change, delete, transfer, user, and data. A plus sign (+) marks the event type for storage, a minus sign (–) excludes the event type from storage. End events cannot be filtered out. This field is enabled when the "Enable Reporting Interface" field is checked.	The data parameter encompasses all event types. *-data* is the default. Each filter criterion must be entered on a separate line, with subsequent lines taking precedence. Examples: *–data* *+change* only *change* and *end* events are stored: *+change* *–data* only *end* events are stored Note that *drop* and *watch* events are sent to clients but are not included with the *+data* filter. Names of data elements in ADU events to be sent to the server are specified with the Eventsink configuration parameter. Each element must be entered on a separate line. If this parameter is not used, all data elements are sent. (The ADUID field is always stored.) Use of wildcards is permitted. Use this parameter with care. Filtering elements from the End event may adversely affect reporting capability.

Persistence tab

Field	Recommended entry	Notes
Enable Persistence	Select to enable the ADU server to offload storage of old ADUs to a database. Otherwise, ignore this field.	ADUs are pushed into the database from the ADU server's memory by the DUStore server. If check pointing is enabled, the ADUs are saved at a regularly specified interval. This is used for failure recovery because ADUs persist across server shutdowns.
Checkpoint frequency (secs)	Enter the minimum interval period in seconds between requests to checkpoint a specified ADU into the DUStore server.	A value of –1 means do not checkpoint.
Lookup Field 1 (indexed)	Enter the name of one of the fields used to index the ADU in the DUStore server.	For example, loginid. Used with the Find method.
Lookup Field 2 (indexed)	Enter the name of one of the fields used to index the ADU in the DUStore server.	For example, queueid. Used with the Find method.
Info Field 1	Enter the name of one of the fields used to identify the ADU in the DUStore server.	For example, type. Used with the Find method.
Info Field 2	Enter the name of one of the fields used to identify the ADU in the DUStore server. Default is media.	For example, media. Used with the Find method.
Info Field 3	Enter the name of one of the fields used to identify the ADU in the DUStore server. Default is site.	For example, site. Used with the Find method.
Info Field 4	Enter the name of one of the fields used to identify the ADU in the DUStore server. Default is blank.	Additional info field with no default value.
Info Field 5	Enter the name of one of the fields used to identify the ADU in the DUStore server. Default is blank.	Additional info field with no default value.

Field	Recommended entry	Notes
Info Field 6	Enter the name of one of the fields used to identify the ADU in the DUStore server. Default is blank.	Additional info field with no default value.
Info Field 7	Enter the name of one of the fields used to identify the ADU in the DUStore server. Default is blank.	Additional info field with no default value.
Info Field 8	Enter the name of one of the fields used to identify the ADU in the DUStore server. Default is blank.	Additional info field with no default value.
Advanced Properties		
Database Search on Create	Enter 1 to enable a DUStore search on the FindOrCreate over the WAN. Default is selected.	
DUStore ADU Batch Size	Controls the number of terminated ADUs that are removed by the server at one time. Default is 50 Minimum is 1	The default value of 50 is recommended for most deployments. Setting this parameter too high results in network congestion problems.

Configuration tab

The following configuration parameters are not presented on the ADU tab in Avaya IC Manager. Set these parameters on the **Configuration** tab.

Property	Recommended entry	Notes
autostart	Specify if the server should automatically start at the same time as the ORB server.	Values: true, false.
timetype	Set ADU server timestamp format.	Value: gmt

Debug tab

The Debug tab does not include any ADU server specific parameters.

Advanced tab

On this tab, you can view the server status by clicking the button next to **Server Status**. For the detail information about Watcher status, you need to use the **`listadu`** command. For more information, see the *Agent Data Unit Server Programmer Guide*.

Alarm server

The Alarm server allows an Avaya IC client or server to generate alarms when there are problems with the system or a component. The Alarm server enables client applications to receive these alarms as events, which allows for intervention by systems personnel or software.

The Alarm server serves three major purposes:

- It receives alarms generated by server and client applications.
- It sends alarms (received as events) to client applications that are interested in obtaining events from one or more sources.
- It supports SNMP trap generation to enable easy integration across the Avaya products into an end-to-end SNMP based management platform.

For details, refer to *Core Services Programmer Guide*.

Note:
If you modify SNMP configuration for the Alarm server, you must restart the Alarm server for these changes to take effect.

This section contains the following:

- General tab on page 429
- Alarm tab on page 429
- Debug tab on page 431

General tab

Field	Recommended entry	Notes
Name	Alarm_*<domain>*	Include the domain in the server name to identify the server.
Domain	Select the Avaya 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 a 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.

Alarm tab

Field	Recommended entry	Notes
Suppress Alarms	Suppresses alarms. Enter in the format: *<alarmname> <minutes> <priority>*	Once an alarm with the given <alarmname> is sent, additional <alarmnames> are discarded for the time specified in <minutes>. After <minutes> have elapsed, the alarm Alarm.RepeatedAlarm is sent with information about the repeated alarm, and the trap is reset. For example, `DS.BadString 15 low` would cause the alarm DS.BadString to be sent once, discarded for 15 minutes, followed by a RepeatedAlarm alarm message with a low priority.
Propagate	Check to have the alarms received by this Alarm server distributed to other Alarm servers. Default is checked.	When enabled, clients assigned to another Alarm server, receive alarms from that Alarm server as well.
Maximum Size of Queue	Specifies the maximum size of the propagation queues. Default is 500.	When the Alarm server receives more alarms than specified here, the oldest alarm in the queue is removed and the new alarm is pushed into the queue.

Field	Recommended entry	Notes
Time threshold for propagation (in min)	Specifies the time threshold in minutes used for propagation. Default is 5.	Alarms older than the specified number of minutes will not be propagated. Using a value of 0 indicates there is no time threshold and all alarms will be propagated.
Enable SNMP	Enables/disables SNMP. Default is unchecked (disabled).	When checked, enables SNMP and generates traps. When unchecked, disables SNMP and does not generate traps. When checked, criteria and all other SNMP properties on the subsequent page are displayed.
Criteria	Specify the filter criteria to use in generating traps for alarm events. Default is *.	For example, enter *priority=emergency* for all emergency alarms. The default value means that traps will be sent for all emergency, high and low alarms. Do not enter quotes because using quotes causes IC Workflow server issues. The Assign and the Monitor methods accept criteria as a parameter.
Trap Sinks	Specify the trap sinks interested in receiving alarm events.	Enter the IP Address of the host and its port number delimited by: For example: *135.157.27.115:500* If the port is not specified, the default port (162) is used. If you enter the IP address and no port, the trap receiver runs on the default port of the machine with that IP address. Do not enter quotes because using quotes causes IC Workflow server issues.
Community	Specify the community used by Master Agent to authenticate SNMPV1/V2c messages. Default is public.	Requests for a different community will not be processed and an authentication failure trap is sent to the requesting NMS.

Field	Recommended entry	Notes
System Contact	Specify the system contact.	A MIB-2 system group object, this is the identification and contact information of the contact person for this managed node. For example, *jsmith@avaya.com* Do not use quotes because using quotes causes IC Workflow server issues.
System Name	Specify the system name.	A MIB-2 system group object, this is the administratively assigned name for this managed node. For example, *AIC_7.1@135.157.27.115* Do not enter quotes because using quotes causes IC Workflow server issues.
Master Agent Port	Enter the UDP port number on which the Master Agent listens and reads SNMP messages. Default is 161.	The UDP port specified here should be available for use. If the specified UDP port is being used by another process, the Master Agent process will not be started and the Alarm server will raise the alarm *SNMP Not Functional*.
Master AgentX Port	Enter the TCP port number on which the Master Agent listens and reads agentx messages from the Subagent. Default is 705.	The TCP port specified here should be available for use. If the specified TCP port is being used by another process, the Master Agent process will not be started and the Alarm server will raise the alarm *SNMP Not Functional*.
Retry Limit	Enter the number of times to try to restart a failed SNMP server.	If the Alarm server fails to start the master agent process, it tries to restart the SNMP server every 10 ms until it completes the specified number of retries. If all retries fail, the Alarm server sends an alarm describing the situation.

Debug tab

The Debug tab does not include any Alarm server specific parameters.

Attribute server

The Attribute server performs the following tasks:

- Acts as a communications bridge between the ICM server and the WebACD server for chat contacts.
- Provides tracking of user Web page browsing sessions for DataWake.
- Provides Website property event notifications between the Website and the ICM server.

This section contains the following:

- General tab on page 432
- Attribute tab on page 433
- Debug tab on page 434

General tab

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 Avaya 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 a system from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

Attribute tab

This server does not have any advanced properties.

Field	Recommended entry
Port	If you must change the default, see IC Installation and Configuration. Port conflicts can cause serious problems within the Avaya IC system.
Enable Datawake Recording	Check this field if: ● The Avaya IC system includes DataWake ● You want this Attribute server to track the Web pages browsed by a Website customer.
Enable ICM Bridge	Check this field.
IC Login	By default, this field uses the `icmbridge` account that is provided with Avaya IC. If you have not already done so, change the default password for this account. **Important:** Do not use the Administrative account for Avaya IC Manager or any other account for which the password may change.
IC Password	Enter the password for the account in the IC Login field.
ICM Servers	● Select the **Ellipsis** (**…**) button. ● In the ICM Servers dialog box: – Select New. – Select Enabled. – Enter the name and domain of the machine that hosts the ICM server. For example, enter TESTBOX.xyzcorp.com. – Accept the default port number or change to an available port. – Select **OK**.
Advanced Properties	
Default WACD Cluster	The cluster name of WebACD. You can only view the name.

Debug tab

You can access the following Attribute server specific debug parameters on the Debug tab.

Field	Recommended entry	Notes
Attribute Server Log File name	Enter the name of the Attribute server log.	The default log file name is `attrsvr.log`.
Attribute Server Log Trace Level	Select a number from 0 to 4, where 0 is the lowest level of logging and 4 is the highest.	The default log level is 2. Because logging requires system resources, you should select a minimal logging level unless you are trying to diagnose a specific problem.
ICM Bridge Log File	Enter the name of the ICM Bridge log file.	The default log file name is `icmbridge.log`.
ICM Bridge Log Level	Select a number from 0 to 4, where 0 is the lowest level of logging and 4 is the highest.	The default log level is 2. Because logging requires system resources, you should select a minimal logging level unless you are trying to diagnose a specific problem.

Blender server

The Blender server controls agent availability across the different channel types and monitors ADU change events. It can be configured to run blending flows when any agent state changes. The Blender server can also be configured to raise alarms or run flows when agent or queue ADU thresholds are exceeded.

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.

This section contains the following:

- General tab on page 435
- Blender tab on page 435
- Watch tab on page 436
- Configuration tab on page 438
- Debug tab on page 438

General tab

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

Blender tab

This server does not have any advanced properties.

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.

Field	Recommended entry	Notes
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.

Watch tab

Field	Notes
Enable watchlist	Select this option to enable the Blender server's watchlist functionality. **Note:** You must first add a Blender server and save it in the Blender tab before enabling the watchlist.
Multiple alarms	If you have enabled the watchlist, you can select this option if you want the Blender server to generate another alarm if a change event's attribute has not changed.
Watch action	The action to take when a watch criterion is met. You can select: – alarmonly - generate an alarm – flowonly - run a flow – alarmandflow - generate an alarm and run a flow

After you enable the watchlist, click **New** to display the Watch Editor where you can define the items you want to watch for. You can specify:

Field	Notes
Type	The type of ADU to be "watched." A pull down menu provides the options, Agent or Queue.
Queue ID	The identifier of the ADU. For a queue, it is the Queue ID. For an agent, it is the agent's login ID.
Site	The physical location of agents, servers, or queues. Avaya IC uses the site information when it makes routing for routing decisions, linking, and call flow optimization.
Media	The media channel upon which the contact was received by Avaya IC.
Flow	The name of the flow to run when a watch criterion is met.
Attribute	The attribute of the ADU to watch. Some of the attributes that may be selected are oldest, abandoned, contact count, contacts handled, and contact offered.
Operator	The comparison operator to use when selecting items to watch. This parameter is used in conjunction with the Value parameter. For example, you can watch the number of contacts handled by the queue or agent by selecting contactcount in the Attributes field. The Op parameter lets you define a limit from which to watch. If you select < (less than) in this field and enter 200 in the following Format parameter. Avaya IC watches the number or contact under 200 for the designated agent or queue.
Value	The value of the attribute to be watched. This parameter can be Value or Time based on the attribute selected in the above parameter. For example, contactcount would have a value format for a number. The oldest attribute would have a time format to indicate its time in Avaya IC.

Configuration tab

The following configuration parameters are not presented on the Blender tab in Avaya IC Manager. Set these parameters on the Configuration tab.

Property	Description	Notes
retry_adu	During startup or in the event of an ADU server failure, the number of times the Blender server should retry assignment to the server before terminating itself.	Value: integer Default: 5
retry_workflow	During startup or in the event of a Workflow server failure, the number of times the Blender server should retry assignment to the server before terminating itself.	Value: integer Default: 10
retry_wait_period	The number of seconds for the Blender server to wait between each retry assignment.	Value: integer Default: 3

Debug tab

The Debug tab does not include any Blender server specific parameters.

CAAdmin (Content Analyzer Administration) server

If you have purchased the optional Avaya Content Analyzer feature of Avaya IC, you need to create an administrative server for your Content Analyzer environment. (If you have not purchased the Content Analyzer feature, this server will not start.)

The Administrative server is used to create, train, and maintain the Content Analyzer Knowledge Bases. When you select an administrative task, Avaya IC checks to see if there is a CAAdmin server already running. If so, it uses that server to perform the task. If not, it randomly selects one (regardless of domain) and attempts to start it. If the attempt is unsuccessful, it tries another one and continues the process until it has tried all of the available servers.

If none of the defined servers starts, Content Analyzer prompts the user to configure a new CAAdmin server.

This domain-independent technique provides a slightly different version of failover than the general failover policy in *IC Administration Guide*. The potential problem is that the selection of the server is completely random, and, if you have multiple CAAdmin servers defined on multiple platforms, the selected server may not have access to the Knowledge Base that you want to work with.

For example, if you create a Knowledge Base called `mykb.kb` and save it to the directory `S:\KBs`, the CAAdmin server saves the Knowledge Base to the physical location that is mapped to the `S` drive on a server system, and it saves the fully-qualified name `S:\KBs\mykb.kb` with the Knowledge Base.

Later on if you want to train that Knowledge Base, Avaya IC either uses the currently-running CAAdmin server or starts one at random. If drive `S` for that new server is not mapped to the same physical location that the original CAAdmin server used, or if the `KBs` directory is not shared between the server systems, then the currently-running CAAdmin server will not be able to access `S:\KBs\mykb.kb`.

Tip:
To avoid this problem, Ensure that all server systems refer to the Knowledge Base storage area in the same way. (For example, if the storage device is mapped to drive `S` on one CAAdmin server, it should be mapped to drive `S` on all of the server systems running a CAAdmin server.)

You should also make sure that this storage location is accessible to the operational CAServer that will be associated with the Knowledge Base. For details, see CA (Content Analyzer) server on page 440.

This section contains the following:

- General tab on page 439
- CAAdmin tab on page 440
- Debug tab on page 440

General tab

Field	Recommended entry	Notes
Name	CAADmin_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya 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 machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

CAAdmin tab

This server does not have any advanced properties.

Field	Recommended entry	Notes
IC Data Source	Select the Interaction Center Data Source.	If you used the default name, select `interaction_center`.

Path to NLP Data	Enter the directory path to the NLP data.	Windows:
		`IC_INSTALL_DIR\etc\oem\banter\nlpdata`
		Unix (Solaris or AIX):
		`IC_INSTALL_DIR\etc\oem\banter\NLPdata`

Debug tab

The Debug tab does not include any CAAdmin server specific parameters.

CA (Content Analyzer) server

If you have purchased the optional Avaya Content Analyzer feature of Avaya IC, you need to create at least one operational Content Analyzer server in your Content Analyzer environment. If you have not purchased the Content Analyzer feature, this server will not start.

The server classifies customer emails at operation time so it must be configured with one or more trained and validated Content Analyzer Knowledge Bases. It must be active whenever you want to process emails coming into the Avaya IC system.

If you make changes to any of the associated Knowledge Bases (such as retraining, synchronization, or renaming), you need to stop this server and restart it so that it picks up the changes.

This section contains the following:

- General tab on page 441
- CAServer tab on page 441
- Debug tab on page 443

General tab

Field	Recommended entry	Notes
Name	OperationCA_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya 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 machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

CAServer tab

This server does not have any advanced properties.

Field	Recommended entry	Notes
IC Data Source	Select the Interaction Center Data Source.	If you used the default name, select `interaction_center`.

Path to NLP Data	Enter the directory path to the NLP data.	Windows:
		`IC_INSTALL_DIR\etc\oem\banter\nlpdata`
		Unix (Solaris or AIX):
		`IC_INSTALL_DIR/etc/oem/banter/NLPData`

Knowledge Base	Enter the name of the Knowledge Base associated with this server.	Select **Knowledge Base** to display the **Knowledge Base** dialog box. For details about entering a Knowledge Base, see below.

To add a Knowledge Base, click **New** on the toolbar and fill in the following fields:

Field	Notes
Name	Enter a name for the Knowledge Base. To avoid confusion, you should use the name that you specified when you created the Knowledge Base in Avaya IC Manager. This is the same Knowledge Base Name as displayed in Knowledge Base Management in IC Managers content analysis administration window.
KB File Location	Enter the fully-qualified location of the Knowledge Base file you created after validation.
Threshold	Leave this blank or set it to the final value you used during validation.
Language	Click the button in this field to display the Language dialog box. Select New and enter the language codes for the languages that you want associated with the Knowledge Base. **Note:** To specify multiple language codes, enter a colon (:) between each code. For example, to specify English, German and French, you would specify `en:de:fr`.

You can use the following language codes:

Language	Code
Chinese, Simplified	zh
English	en
French	fr
German	de
Italian	it
Japanese	ja
Korean	ko
Portuguese	pt
Spanish	es

Debug tab

The Debug tab does not include any CAServer server specific parameters.

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.

This section contains the following:

- General tab on page 444
- ComHub tab on page 444
- Debug tab on page 445

General tab

Field	Recommended entry	Notes
Name	Comhub_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya 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 machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

ComHub tab

This server does not have any advanced properties.

Field	Recommended entry	Notes
Host Name	Enter the fully-qualified domain name of the machine that hosts the ComHub server.	For example, enter TESTBOX.xyzcorp.com.
Service Port	Accept the default port of 4001 or enter a new port.	If you must change the default, see IC Installation and Configuration. 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`.
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.

Debug tab

You can access the following ComHub server specific debug parameters on the Debug tab.

Field	Recommended entry	Notes
Data Query Log Level	Select a number from 0 to 4, where 0 is the lowest level of logging and 4 is the highest.	The default log level is 3. Because logging requires system resources, you should select a minimal logging level unless you are trying to diagnose a specific problem.
Log Device Filename	Enter the name of the Log Device file.	The default log file name is `../logs/wcservlet.log`.
Comhub Log Filename	Enter the name of the Comhub server log.	The default log file name is `../logs/comhub.log`.

Data server

The Data server monitors and processes requests between Avaya applications and their databases. The Data server lets you create database-independent applications using the Data server's libraries instead of database libraries.

The Data server provides database independence for Avaya applications because the connection information that is stored in the IC Data Source determines which database the application connects to and which style of SQL to generate.

In the Interaction Center 7.3.x, the Data server can be configured to operate with several databases. For details, refer to *Core Services Programmer Guide* and *IC Installation Planning and Prerequisites*.

Note:
If the database is down for 30 minutes or more, you must shutdown the IC Data server.

This section contains the following:

- General tab on page 446
- Debug tab on page 446
- DataServer tab on page 446
- DataServer tab for IBM DB2 on page 447
- DataServer tab for MSSQL Server on page 448
- DataServer tab for Oracle on page 450

- DataServer tab for ODBC on page 452

General tab

Field	Recommended entry	Notes
Name	Enter a logical name for the Data server. For example: • DataServerMSSQL • DataServerOracle • DataServerDB2 • DataServerODBC	Include the type of database on your Avaya IC system in the name. You need this name to configure IC Repository database. **Tip:** For all secondary Data servers, include the domain in the server name to identify the server.
Domain	Select the Avaya 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 machine that hosts the server, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

Debug tab

The Debug tab does not include any Data server specific parameters.

DataServer tab

Use the following DataServer tab that corresponds to the database for which you are configuring the Data server.

- DataServer tab for IBM DB2 on page 447
- DataServer tab for MSSQL Server on page 448
- DataServer tab for Oracle on page 450
- DataServer tab for ODBC on page 452

DataServer tab for IBM DB2

The settings on this tab pertain to the Data server using an IBM DB2 database.

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.
Advanced Properties		
Database Connection Timeout (min)	Enter the number of minutes after which the Data server closes an inactive database connection. Default is 10.	Prevents an inactive database connection from remaining allocated.
DB Heart Beat Interval (min)	Enter the number of minutes at which to poll the system for database connectivity. Default is 1.	The number of minutes at which the system checks to see if the database is still up and running or detects that it is down.

Field	Recommended entry	Notes
DB Retry Interval (sec)	Enter the number of seconds after which the Data server should try to reconnect to the database after detecting a connectivity problem. Default is 5.	If the system finds the database is down, the interval (seconds) at which the system checks to see if the database is back up and running.
Warning Levels (on/off)	Check this field to enable the Data server to check for certain warnings. Default is unchecked.	If checked, the server checks for the following warnings: ● High record count ● High SQL execution time ● High queried time (waiting time in the Data server)

DataServer tab for MSSQL Server

The settings on this tab pertain to the Data server using a MSSQL Server database.

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.
SQL Driver (Windows Only)	Select an appropriate ODBC driver.	This field is introduced in IC 7.3.3. The drop-down list displays only the ODBC drivers that you installed on the system. ● Blank (No value) ● SQL Server ● SQL Server Native Client 10.0 ● SQL Server Native Client 11.0 If the Blank (no value) is selected, then the value from the Database Designer is selected.

Field	Recommended entry	Notes
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.
Advanced Properties		
Database Connection Timeout (min)	Enter the number of minutes after which the Data server closes an inactive database connection. Default is 10.	Prevents an inactive database connection from remaining allocated.
DB Heart Beat Interval (min)	Enter the number of minutes at which to poll the system for database connectivity. Default is 1.	The number of minutes at which the system checks to see if the database is still up and running or detects that it is down.
DB Retry Interval (sec)	Enter the number of seconds after which the Data server should try to reconnect to the database after detecting a connectivity problem. Default is 5.	If the system finds the database is down, the interval (seconds) at which the system checks to see if the database is back up and running.
DB Login Timeout (in seconds)	Enter the period of time, in seconds, after which the Data server's open connection request to the database will timeout if the database does not respond within that time period. Default is 60.	MSSQL Server only

Field	Recommended entry	Notes
DB Query Timeout (in seconds)	Enter the period of time, in seconds, a SQL operation at the database will timeout if the database does not respond within this time period. Default is 60.	MSSQL Server only
Warning Levels (on/off)	Check this field to enable the Data server to check for certain warnings. Default is unchecked.	If checked, the server checks for the following warnings: ● High record count ● High SQL execution time ● High queried time (waiting time in the Data server)

DataServer tab for Oracle

The settings on this tab pertain to the Data server using an Oracle database.

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.
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 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.

Field	Recommended entry	Notes
Advanced Properties		
Database Connection Timeout (min)	Enter the number of minutes after which the Data server closes an inactive database connection. Default is 10.	Prevents an inactive database connection from remaining allocated.
DB Heart Beat Interval (min)	Enter the number of minutes at which to poll the system for database connectivity. Default is 1.	The number of minutes at which the system checks to see if the database is still up and running or detects that it is down.
DB Retry Interval (sec)	Enter the number of seconds after which the Data server should try to reconnect to the database after detecting a connectivity problem. Default is 5.	If the system finds the database is down, the interval (seconds) at which the system checks to see if the database is back up and running.
Warning Levels (on/off)	Check this field to enable the Data server to check for certain warnings. Default is unchecked.	If checked, the server checks for the following warnings: • High record count • High SQL execution time • High queried time (waiting time in the Data server)

DataServer tab for ODBC

The settings on this tab pertain to the Data server using an ODBC database.

Field	Recommended entry	Notes
DB Login	Enter the ODBC database 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.
Advanced Properties		
Database Connection Timeout (min)	Enter the number of minutes after which the Data server closes an inactive database connection. Default is 10.	Prevents an inactive database connection from remaining allocated.
DB Heart Beat Interval (min)	Enter the number of minutes at which to poll the system for database connectivity. Default is 1.	The number of minutes at which the system checks to see if the database is still up and running or detects that it is down.
DB Retry Interval (sec)	Enter the number of seconds after which the Data server should try to reconnect to the database after detecting a connectivity problem. Default is 5.	If the system finds the database is down, the interval (seconds) at which the system checks to see if the database is back up and running.

Field	Recommended entry	Notes
SQL query to fetch DateTime	Specify an alternate SQL for fetching datetime from the ODBC database.	This overrides the default ODBC SQL, which is: SELECT DISTINCT {fn NOW() FROM qw_keys
Warning Levels (on/off)	Check this field to enable the Data server to check for certain warnings. Default is unchecked.	If checked, the server checks for the following warnings: • High record count • High SQL execution time • High queried time (waiting time in the Data server)

Directory server

The Configuration tab on page 456 (DS) provides a common directory of resources that are available in Avaya IC. Directory entries include users, Telephony servers, telephony resources, and other logical and physical elements. The DS also stores agents, queues, and workgroups in the database.

For details, refer to *Core Services Programmer Guide*.

This section contains the following:

- General tab on page 453
- Directory tab on page 454
- Configuration tab on page 456
- Advocate tab on page 457
- Debug tab on page 457

General tab

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.

Field	Recommended entry	Notes
Host	Select the machine's IP address from the drop-down list, or enter a new IP address.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.
AutoStart	Select the check box for this property.	Automatically starts the Directory server when you start the machine.

Directory tab

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	Check this box if this Directory server will be 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 used a backup copy of the directory. Click the Start button to create the file in the server's home directory.	Avaya IC appends an .ffd extension to the file name.
Restore	Enter file name of the backup file used as the name of the directory you want to restore. Click the Start button 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 small 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.

Field	Recommended entry	Notes
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.
Certificate File	Default value: domain_cert_AvayaIC_Server.pem.	Directory Server SSL certificate file name. The file is in the .PEM format.
Key File	Default value: domain_key_AvayaIC_Server.pem.	Directory Server SSL Certificate Private Key file name.
SSL Socket Port	Default value: 14433.	Port to be used for SSL communication for accepting the login request.
Advanced Properties		
Update LDAP Config on Generic Update	By default, the check box is not selected.	Select the check box to update the Directory server properties, related to the IC and LDAP integration, at run time, through generic update.
DHParam File	Keep the default value.	This parameter is not used currently. A warning message about the missing `dh1024.pem` file is logged in to Directory Server log. This option is created for future implementation.

Configuration tab

The following configuration parameters are present on the Configuration tab on the Directory server in Avaya IC Manager. Set these parameters on the **Configuration** tab.

Field	Recommended entry	Notes
TimeWindowFor MaxFailedLogin Attempts	Default: 60 seconds	Time in seconds within which if M (MaxFailedLoginAttemptsInTime) successive failed login attempts are made an alarm is raised.
MaxFailedLogin AttemptsInTime	Default: 3	Number of successive login failures within the specified time in seconds (TimeWindowForMaxFailedLoginAtt empts)

Note:
You must reconfigure the repository database after installing IC 7.3.5 FP.

If IC Repository database is not reconfigured, then system raises alarms after 10 login attempts and after the 25th login attempt, all logins are disabled.

If logins are disabled, perform the following steps:

1. Reconfigure repository database.
2. Restart or update the Directory Server.

SSL configuration parameters for compatibility with earlier versions of IC

A client from an older version of IC (IC 7.3.3 and IC 7.3.4) cannot communicate with an upgraded IC 7.3.5 DS for 'Login' or 'Authenticate' requests. To enable communication during upgrade scenarios, use the following new hidden configuration parameters:

Field	Recommended entry	Notes
TLSProtocol	Default: TLS 1.2 For compatibility with earlier IC versions use the following versions: TLS 1.0	This configuration variable is provided for backward compatibility.
CipherList	ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2	This configuration variable allows user to set new CIPHER list.

To configure above properties, atleast one IC Manager system should be upgraded to release 7.3.5. The property added must be removed when all the clients are upgraded to IC 7.3.5.

Configuration parameter allow_sslv3 is obsolete and must be removed from the configuration, if added when IC is upgraded to 7.3.5.

Note:
SSLv3 is no longer supported from IC Release 7.3.5.

IC Clients (for example AARC, and so on) releases prior to 7.3.3 FP will not work with IC release 7.3.5.

Change in SSL communication (Introduced in IC 7.3.5)

- OpenSSL library is upgraded to version 1.0.x.
- IC SSL/TLS enabled severs, for example, Directory Server (DS), HTTPConnector Server are modified from IC 7.3.5 FP onwards to accept only TLSv1.2 during TLS handshake.

IC SSL/TLS clients, for example, AARC, AAWC now uses TLSv1.2 during TLS handshake.

Advocate tab

Field	Recommended entry	Notes
Enable Advocate	Select this check box to enable the optional Avaya Business Advocate feature. **Note:** Before you check this field, ensure that the Business Advocate database has been created and the DB connection has been properly configured. (For details, see *IC Database Designer Application Reference*.)	Avaya Business Advocate is a resource management tool that routes contacts through work distribution intelligence.

Debug tab

The Debug tab does not include any Directory server specific parameters.

DUStore server

The DUStore server manages the DUs (EDUs and ADUs) that are created by Avaya IC. DUStore can store all types of DUs, but most of the time only Email DUs are stored. This is because email tasks can remain inactive for long periods of time. The DUStore server interfaces to a database of inactive EDUs. It stores the EDUs in the database in their entirety. When an EDU server method is invoked for an EDU that is no longer in memory, the DUStore server restores the EDU as if it were assigned to an active contact.

For details, refer to *Electronic Data Unit Server Programmer Guide*.

This section contains the following:

- General tab on page 458
- DUStore tab on page 459
- Debug tab on page 459

General tab

Field	Recommended entry	Notes
Name	DUStore_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya 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 email contacts. For details about recommended domains, see *IC Installation Planning and Prerequisites*.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

DUStore tab

Field	Recommended entry	Notes
IC Data Source	Select the IC Data Source, which is the ADL file, for the 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 absence of other information. Default is 60 days.	Avaya ICAfter 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.	
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 (this interval + 1) to start.
Purge Alarm	Check to raises an alarm if a delete scan finds any EDUs that meet the criteria for deletion and retirement to the database. Default is checked.	
Advanced Properties		
Table	Enter the name of the table in which the DU data is stored.	

Debug tab

The Debug tab does not include any DUStore server specific parameters.

EAI server

The EAI server is only used when you integrate Siebel with Avaya IC. For details, see *Avaya IC for Siebel Integration*.

EAI Email server

The EAI Email server is only used when you integrate Siebel with Avaya IC. For details, see *Avaya IC for Siebel Integration Guide*.

EAI Workflow server

The EAI Workflow server is only used when you integrate Siebel with Avaya IC. For details, see *Avaya IC for Siebel Integration Guide*.

EDU (Electronic Data Unit) server

The EDU server creates, stores, and manages EDUs on Avaya IC. It creates EDUs in response to requests from Avaya servers and client applications. The EDU server manages an EDU throughout its lifecycle. It stores open EDUs, records events, and provides services that enable clients to interact with a contact.

When adding a new EDU server to Avaya IC in Avaya IC Manager, the **Initialize EDU** dialog is displayed. Designate the media type for which to optimize the EDU server from one of the following:

- Voice
- Chat
- Email

For details, refer to *Electronic Data Unit Server Programmer Guide*.

This section contains the following:

- General tab on page 461
- EDU tab on page 462

- Persistence tab on page 467
- Debug tab on page 468

General tab

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, enter EDU_Voice1_Voice.
Domain	Select the Avaya IC domain for the server from the drop-down list.	The domain for the EDU server depends upon which channel the EDU server handles. For voice contacts, add the EDU server to the same domain as the associated Telephony server. For chat 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 details about recommended domains, see *IC Installation Planning and Prerequisites*.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

EDU tab

Field	Recommended entry	Notes
Idle Time (min)	Enter the maximum length of time, in minutes, that Avaya IC should maintain an EDU record if a contact is idle. Default varies by channel: voice = 60 email = 30 chat = 45	Make sure that the number of minutes entered in this field is greater than the length of a typical contact. Minimum is 1 minute Maximum is 15 hours
No User Interval (sec)	Enter the minimum number of seconds an EDU may reside in memory when there are no users active for it. Default varies by channel: voice = 1,800 email = 120 chat = 90 Minimum is 1 second, Maximum is 60 minutes.	Very low values may cause thrashing if cooperating applications allow any gap passing EDUs among themselves.
Random Kill Interval (sec)	Enter the maximum number of seconds an EDU stays in memory after the usual timers have expired. Default varies by channel: voice = 30 email = 120 chat = 60	Random intervals are useful when a large number of EDUs are simultaneously terminated causing the IC Repository and the DUStore server to be flooded with requests. Handling the requests over a 2-minute period decreases database server stress. In situations where this is unlikely, more predictable timing and better memory usage result from a setting of 1. While testing to see if EDUs are being retired when they should be, 1 is also an appropriate setting.
Scan Interval (sec)	Enter the number of seconds to wait between checking various EDU server timers. Default varies by channel: voice = 4 email = 3 chat = 6	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 (this interval + 1) to start.

Field	Recommended entry	Notes
Max Active EDUs	Enter the maximum number of EDUs that the EDU server keeps active at the same time. Default varies by channel: voice = 2,048 email = 4,096 chat = 2,048	If more than this number of EDUs are created, the EDU server sends an alarm and forcibly terminates the oldest one to make room for each new one.
Allowed Assigns	Enter the number of clients interested in assigning to EDU servers. Default is 8,192 for all channels.	To start, this should be equal to the number of agents in the contact center (or across all contact centers in a WAN environment), plus a few extra.
Pool Size	Enter the initial amount of memory allocated for data belonging to each EDU. Default varies by channel: voice = 8,000 email = 5,000 chat = 10,000	Increase the pool size if a large amount of data is stored and performance needs to be improved.
Advanced Properties		
Enable Reporting Interface	Check to enable reporting. Default is checked for all channels.	Checking this field displays the "filter" parameter, which is described at the end of this table.
Pool Growth Increment	Enter the amount of memory (in mg) by which to increase pool size allocation when more memory is needed to store strings or events. Default is 1024 for all channels.	
Initial Number of Fields	Enter the number of fields expected in an EDU. Default is 128 for voice and email, 256 for chat. If using containers, increase this value to 256 or 512.	This parameter does not limit the number of fields, but when this number is exceeded, the server must reallocate space.

Field	Recommended entry	Notes
Pool Re-Pack (%)	Specify the percentage of memory that is free in the ADU pool, when the ADU server will repack the pool to save memory. Default varies by channel: voice = 20 email = 15 chat = 10	Sites at which performance is critical and memory is plentiful should consider using a value of 100.
Poll Wait (ms)	Enter the interval value, in hundredths of a second, for the IC Toolkit's Select() method. Default value is 2 (ms) for all channels.	Low values increase CPU utilization. High values (over 100) may affect the accuracy of the scaninterval parameter.
Maximum Number of Revisions	Enter the number of revisions of a value kept for access with the GetValuesHistory() method. Default is 1 for all channels, which is recommended.	Caution: Do not enter 0 in this field. If this 0 is entered, the EDU server keeps all revisions, which could result in a failure due to lack of system resources.
Maximum Number of Cached EDU events	Enter the maximum number of events to be kept in memory for each EDU. Default varies by channel: voice = 128 email = 64 chat = 192	A setting of 64 is recommended as a reasonable number of events to be kept in memory. High values may increase Eventsink throughput. Low values may conserve memory.
Subcontainer Instances	Enter the number of instances of a subcontainer created with the + token that can exist at one time, in the format <containername>.<integer>. If more instances than this number are created, the earliest instance is deleted. Default is 0, which specifies no limit (all instances of a subcontainer are kept). A setting of 4 is recommended.	Exampled limit the number of subcontainers of the ts container, set gencount to voice.3. When voice.+ creates voice.4, voice.1 is deleted. When voice.5 is created, voice.2 is deleted and so on. The gencount must be set for the "voice", "chat", and "email" containers on the Configuration tab using the following name/value pairs: "gencount", "voice.4" "gencount", "chat.4" "gencount", "email.4"

Field	Recommended entry	Notes
Retry Interval (sec)	Enter the number of seconds to wait between automatic attempts to reassign to IC servers. Default is 60 (1 minute) for all channels. Minimum is 6 seconds Maximum is 172800 seconds (48 hours)	It is not recommended to set this value below 30 seconds in a production environment. It performs a synchronous DS call for a list of EDU servers and attempts an asynchronous Assign to any of them that it isn't already assigned to. If the Assign fails (the request function itself fails), the offending EDU server is removed from the list and not retried automatically. The retry is only attempted if the Assign callback reveals an error or a ServerFailed event arrives.
Reset Interval (sec)	Enter the number of seconds to wait between attempts to reassign to servers after receiving a VDU.FailVDUCon alarm. Default is 2 seconds for all channels. Minimum is 0 Maximum is 172800 seconds (48 hours)	
Data Element Names	Enter the names of the data elements in EDU events to be sent to the server specified on the Event Sink option.	Enter each element on the Edit dialog. If this option is not set, all data elements are stored. The EDUID field is always stored. The use of wildcards is permitted. Use this parameter with care; filtering elements from the End event may adversely affect reporting capability.
Suspend Interval (sec)	Enter the number of seconds before an EDU, which is suspended by use of the Suspend method by all users, is considered for Suspension. Default is 30 seconds for all channels. Minimum is 1 Maximum is 1200 seconds (20 minutes).	This parameter can be overridden by a higher value in the Suspend method.

Field	Recommended entry	Notes
EDU Data Percent	Enter the percentage of EDUs sent to the EDU data feed to be used for random sampling. Default is 0 for all channels. Minimum is 0 Maximum is 100	
Filter	Set the filter to determine which EDU events are sent to the Report server. Event types are start, change, delete, transfer, user, and data. A plus sign (+) marks the event type for storage, a minus sign (–) excludes the event type from storage. End events cannot be filtered out. This field is enabled when the "Enable Reporting Interface" field is checked.	The data parameter encompasses all event types. *-data* is the default. Each filter criterion must be entered on a separate line, with subsequent lines taking precedence. Examples: *–data* *+change* only *change* and *end* events are stored: *+change* *–data* only *end* events are stored Note that *drop* and *watch* events are sent to clients but are not included with the *+data* filter. Names of data elements in ADU events to be sent to the server are specified with the Eventsink configuration parameter. Each element must be entered on a separate line. If this parameter is not used, all data elements are sent. (The ADUID field is always stored.) Use of wildcards is permitted. Use this parameter with care. Filtering elements from the End event may adversely affect reporting capability.

Persistence tab

Field	Recommended entry	Notes
Enable Persistence	Select to enable the EDU server to off load storage of old EDUs to a database. Avaya recommends you do this for email, but not for voice and chat.	EDUs are pushed into the database from the EDU server's memory by the DUStore server. If check pointing is enabled, the EDUs are saved at a regularly specified interval. This is used for failure recovery because EDUs persist across server shutdowns.
Advanced Properties		
Checkpoint frequency (secs)	Enter the minimum interval period in seconds between requests to checkpoint a specified EDU into the DUStore server.	A value of –1 means do not checkpoint.
Persistence Service Name	Enter the name assigned to the Persistence server used by the EDU server. Default is DUStore.	
Database Search on Create	Check to enable a DUStore search on the FindOrCreate over the WAN. Default is checked.	
Lookup Field 1 (indexed)	Enter the name of one of the fields used to index the EDU in the DUStore server.	For example, loginid. Used with the Find method.
Lookup Field 2 (indexed)	Enter the name of one of the fields used to index the EDU in the DUStore server.	For example, queueid. Used with the Find method.
Info Field 1	Enter the name of one of the fields used to identify the EDU in the DUStore server.	For example, type. Used with the Find method.
Info Field 2	Enter the name of one of the fields used to identify the EDU in the DUStore server. Default is media.	For example, media. Used with the Find method.

Field	Recommended entry	Notes
Info Field 3	Enter the name of one of the fields used to identify the EDU in the DUStore server. Default is site.	For example, site. Used with the Find method.
Info Field 4	Enter the name of one of the fields used to identify the EDU in the DUStore server. Default is blank.	Additional info field with no default value.
Info Field 5	Enter the name of one of the fields used to identify the EDU in the DUStore server. Default is blank.	Additional info field with no default value.
Info Field 6	Enter the name of one of the fields used to identify the EDU in the DUStore server. Default is blank.	Additional info field with no default value.
Info Field 7	Enter the name of one of the fields used to identify the EDU in the DUStore server. Default is blank.	Additional info field with no default value.
Info Field 8	Enter the name of one of the fields used to identify the EDU in the DUStore server. Default is blank.	Additional info field with no default value.
DUStore EDU Batch Size	Controls the number of terminated EDUs that are removed by the server at one time. Default is 50 Minimum is 1	The default value of 50 is recommended for most deployments. Setting this parameter too high results in network congestion problems.

Debug tab

The Debug tab does not include any EDU server specific parameters.

Event Collector server

The Event Collector server collects many types of data from ADU servers, including agent data, queue data, service class data, and outbound job statistics.

Each Event Collector server has a one-to-one relationship with the associated Avaya OA real-time subsystem to which it sends data. If you have more than one real-time subsystem, you need more than one Event Collector server.

For details about this server, see *Operational Analyst Installation and Configuration*.

This section contains the following:

- General tab on page 469
- EventCollector tab on page 470
- Debug tab on page 471

General tab

Field	Recommended entry	Notes
Name	EventCollector_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select 0A from the drop-down list if the server is in the OA domain.
Host	Select the IP address of a system from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

EventCollector tab

This server does not have any advanced properties.

Field	Recommended entry	Notes
Site	Select the site where this server is located from the drop-down list.	The Event Collector server must be in the same site as the Telephony Queue Statistics server (or servers) from which the Event Collector server collects Telephony Server Queue statistics.
Domains to Monitor	Click the **Ellipsis (…)** button and in the Domains to Monitor dialog box: ● Click the >= button. ● From the drop-down list, select a domain. ● Repeat to select all the required domains. ● Click **OK**.	The list of monitored domains for an Event Collector server must include all the domains at the site that contain agents and all the domains containing ADU servers that monitor agents at the site. For example, if the agents at site taos are configured to be in domains taos_user1 and taos_user2, and the ADU servers monitoring those agents are in domains taos_voice1 and taos_voice2, then the Event Collector for site taos must be configured to monitor domains taos_user1, taos_user2, taos_voice1, and taos_voice2. The order that the domains are listed does not matter. Do not add the same domain twice. This will cause errors in the Avaya OA historical data.
Real-Time System ID	Enter the Real-time System ID associated with the real time system that receives data from this Event Collector server.	Real-time System IDs are numeric values that a system administrator assigns and associates with a Real-time subsystem. For details, see *Operational Analyst Installation and Configuration*. **Caution:** If the Avaya IC system includes more than one Event Collector server, do not use the same value for the Real-time System ID. If you assign the same value, the connection to the servers cannot stay active.

Field	Recommended entry	Notes
Data Manager Host	Enter the Data Manager Host for this Event Collector server.	This is the name or IP address of the machine that hosts the Avaya OA Real-time system that receives data from this Event Collector server. **Caution:** If the Avaya IC system includes more than one Event Collector server, do not use the same value for the Data Manager Host. If you assign the same value, the connection to the servers cannot stay active.
Agent Availability Algorithm	Select the Agent Availability Algorithm to be used for this Event Collector server.	An Event Collector server can use one of the following algorithms: ● AGENT_LOAD_BASED (for agent load) ● CHANNEL_LOAD_BASED (for media channel load).
Monitor WAA	Do not check this box unless the Avaya IC system includes Business Advocate for chat contacts or email contacts.	For Business Advocate only. Specifies whether this Event Collector server listens to service class details for chat contacts or email contacts. Only one Event Collector server in Avaya IC system can monitor the WAA. Avaya recommends that you locate this Event Collector server at the same site as the WAA server.

Debug tab

The Debug tab does not include any Event Collector server specific parameters.

Event Collector Bridge server

The Event Collector Bridge server functions as a gateway between the Event Collector server and Business Advocate. This server queries Business Advocate data and collects Business Advocate administration events that are published to Microsoft Message Queuing (MSMQ) by Business Advocate. The server sends this data to the Event Collector server, which forwards the data to the Avaya OA Real-time subsystem to support real-time and historical reporting requirements.

For details about this server, see *Operational Analyst Installation and Configuration*.

This section contains the following:

- General tab on page 472
- Event Collector Bridge tab on page 473
- Debug tab on page 473

General tab

Field	Recommended entry	Notes
Name	ECB_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select 0A from the drop-down list if the server is in the OA domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

Event Collector Bridge tab

This server does not have any advanced properties.

Field	Recommended entry	Notes
Advocate Host	Enter the name of the primary Business Advocate host system.	This is the host name as known to the MSMQ subsystem for the first installed Logical Resource Manager. **Important:** Do not use an IP address for the Business Advocate host name.

Debug tab

The Debug tab does not include any Event Collector Bridge server specific parameters.

HTTP Connector server

With the HTTP Connector, Avaya IC server can make HTTP requests over TCP sockets and serves Prompter pages.

The HTTP Connector server is a generic HTTP interface server. The HTTP Connector server can also communicate securely with SSL enabled clients.

This section contains the following:

- General tab on page 474
- Configuration tab on page 474
- HTTPConnector tab on page 475
- Debug tab on page 477

General tab

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

Configuration tab

A client from an older version of IC (IC 7.3.3 and IC 7.3.4) cannot communicate with an upgraded IC 7.3.5 DS for 'Login' or 'Authenticate' requests. To enable communication during upgrade scenarios use the following new hidden configuration parameters:

Field	Recommended entry	Notes
TLSProtocol	Default: TLS 1.2 For compatibility with earlier IC versions use the following versions: TLS 1.0	This configuration variable is provided for backward compatibility.
CipherList	ALL:!aNULL:!eNULL:!ADH:!EXP:!MD5:!RC4:+HIGH:+MEDIUM:-LOW:-SSLv2	This configuration variable allows user to set new CIPHER list.

To configure above properties, atleast one IC Manager system should be upgraded to release 7.3.5. The property added must be removed when all the clients are upgraded to IC 7.3.5.

Configuration parameter allow_sslv3 is obsolete and must be removed from the configuration, if added when IC is upgraded to 7.3.5.

Note:
SSLv3 is no longer supported from IC Release 7.3.5.

IC Clients (for example AARC, and so on) releases prior to 7.3.3 FP will not work with IC release 7.3.5.

Change in SSL communication (Introduced in IC 7.3.5)

- OpenSSL library is upgraded to version 1.0.x.
- IC SSL/TLS enabled severs, for example, Directory Server (DS), HTTPConnector Server are modified from IC 7.3.5 FP onwards to accept only TLSv1.2 during TLS handshake.
- IC SSL/TLS clients, for example, AARC, AAWC now uses TLSv1.2 during TLS handshake.

HTTPConnector tab

This server does not have any advanced properties.

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`.
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 *`AVAYA_IC_HOME`*.
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	By default the check box is not selected.	Select the check box if you want the HTTPConnector server securely communicate with SSL enabled clients.

Field	Recommended entry	Notes
Certificate File	domain_cert_AvayaIC_Server.pem. This is a self signed certificate.	HTTPConnector Server certificate file name. You can use either self signed (CA) certificate or generate a server certificate using any CA. For example, Verisign. The certificate file should be in the `.PEM` format. You can view this field only when you select the **Enable SSL** check box.
Key File	domain_key_AvayaIC_Server.pem.	HTTPConnector Server Certificate Private Key file, which is used with the server certificate. You can view this field only when you select the **Enable SSL** check box.
HTTPS Port	Default value: 9170.	Port to be used for SSL communication for accepting the login request. You can view this field 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 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. **Note:** If you are running multiple HTTPConnector servers on the same machine, ensure that they use different ports.

Field	Recommended entry	Notes
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 did not receive any response from the agent within this time interval. The default is 600 seconds.

Debug tab

The Debug tab does not include any HTTP Connector server specific parameters.

HTTPVOX server

The HttpVOX Server provides connection from Interaction Center (IC) to Voice Portal (VP) using the HTTPConnector Server. The role of HttpVOX server is to process the requests coming from Voice Portal.

HttpVOX server processes the requests coming from VP or IR over the HTTP Protocol. HTTP based architecture enables scalability and seamless failover support because the HTTP Protocol is loosely coupled, stateless and connection less. A request can go to any server making it highly load balanced and available opposed to traditional socket based architecture used in VOX, where if one VOX server goes down, another VOX server has to be manually restarted.

When using HttpVOX for integrating VP or IR with IC, Speech Applications for gathering caller information can be created using Dialog Designer (DD), a tool for creating speech and/or call control applications that comply with VoiceXML or CCXML specifications. Designed as an Eclipse plug-in, DD provides an integrated GUI for the design and implementation of speech applications that can operate with VP and IR systems.

The HttpVOX server integrates with DD using the HTTPConnector Server. HttpVOX is tested with 200 ports over a volume of 12000 calls per hour.

Note:
HttpVox server is compliant with the `E.164` based dial plan.

This section contains the following:

- General tab on page 478
- HttpVOX tab on page 479
- Debug tab on page 481
- Advanced tab on page 481

General tab

Field	Recommended entry	Notes
Name		Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the HttpVOX server.	
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, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

HttpVOX tab

Field	Recommended entry	Notes
VRU Port Extensions/VDNs		Click the button to add a single extension number of a range of extension numbers. **Note:** HttpVOX supports up to 12 digits as the maximum extension length.
Enable Extended Data Support		If you select the **Enable Extended Data Support** check box, the HttpVOX server extracts the extended UUI data from the `TS.IncomingCall` event and send that data to Telephony Server while transferring the call using TS.TransferEx method. If you do not select the **Enable Extended Data Support** check box, the HttpVOX server still calls the **TS.TransferEX** method with NULL extended data.
Create EDUs	Select the check box if you want the call to connect to Voice Portal first.	You must select the **Create EDUs** check box, if your call is connecting to Voice Portal first because in this case, the HttpVOX Server creates the EDUID and returns that EDUID to Voice Portal.
Network IVR	Select the check box if you want the call to connect to Voice Portal first.	

Field	Recommended entry	Notes
pseudo-ANIs		In the pseudo-ANIs field, you can specify a single number or a range of numbers separated by a hyphen. For example, 100-102. Before Voice Portal transfers the call to Interaction Center, the Dialog Designer application takes the value specified in the **pseudo-ANIs** field and sends that value to Telephony server. If pseudo-ANI value is present with the Telephony server, Telephony server does not create the EDUID and sends a request to the HttpVOX server for sending the EDUID related to that pseudo-ANI. For more information about pseudo-ANIs, see the *Avaya IC integration with VP / IR Guide*. Note: You can see the **pseudo-ANIs** field only if you select the **Network IVR** check box.
pseudo-ANI Timeout (sec)		The value in the **pseudo-ANI timeout (sec)** field is the time for which the HttpVOX server waits for the Dialog Designer to take the value specified in the **pseudo-ANI** field. Note: You can see the **pseudo-ANI Timeout (sec)** field only if you select the **Network IVR** check box.

Configuration tab

Property	Recommended entry	Notes
CTI Type		Format of the parameter: • Couple Contains a name and a value. • Sequence Contains a comma separated list of couples.
Name	adu_update_interval	
Value	10	The HttpVOX server checks all the ADUIDs that it creates for each extension at every interval that you specify in the `adu_update_interval` parameter. The `adu_update_interval` parameter ensures that no ADUID Reaches the IDLE time.

Debug tab

The Debug tab does not include any HTTPVOX server specific parameters.

Advanced tab

On this tab, you can view the HTTPVox server status information by clicking the **Server Status** button.

Email server

The IC Email server interacts with Poller and SMTP servers for polling and forwarding of emails into the Avaya 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 contains the following:

- General tab on page 482
- Configuration tab on page 485
- Debug tab on page 485

General tab

Field	Recommended entry	Notes
Name	Email_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	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, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

ICEmail tab

You can set the following parameters on the ICEMail tab (to view the advanced properties listed below, right-click and select Show Advanced Properties from the pop-up menu):

Field	Recommended entry	Notes
IC Data Source	Select the Interaction Center Data Source.	If you used the default name, select `interaction_center`.
Run Analyze Flow	Select this field.	Check 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 the *Avaya IC Media Workflow Reference*.
Run Outbound Email Flow	For the initial installation of Avaya IC, clear this field.	Select this field if you want to: ● Have Avaya IC analyze outbound email. ● Have an approver 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 computer, ensure that the port number is different for each IC Email server.

Field	Recommended entry	Notes
Template Admin Port	Accept the default or change if required.	Specifies the port on which the built-in HTTP server will listen. This is the port that is used if the specific server ports are not set. If this value is 0, the port defaults to the value set in the advanced property: HTTP Port for Admin Interface. If you must change this port, see *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 computer, ensure that the port number is different for each IC Email server.
Advanced Properties		
Database Query Retries	Accept the default or change, if required.	Determines the maximum number of times that the IC Email server will retry database queries if they fail. If this number of retries is exceeded, the IC Email server will shut itself down.
Analyze Flow Timeout (sec)	300	The length of time that the server should wait before sending another Analyze event.
Outbound Email Flow Timeout (sec)	300	The length of time that the server should wait before sending another Outbound Email event.
Process Request Threads	5	The number of threads per load that should be run to process VESP requests.
Process Events Threads	1	The number of threads that should be run to process events sent to the server.
IC Server Retry Interval (sec)	10	The length of time that the server should wait if a VESP request fails before trying again.

Field	Recommended entry	Notes
Email Threads	10	The number of threads that can process email objects concurrently on the IC Email server state system.
Populate "Reply-To" in Outbound emails	By Default, this check-box is not selected. By Default, this settings adds the return address configured in polling account to the **From** address field of an outbound email.	When you select this check-box, for an outbound email, the system uses the return address configured in the polling account header to populate the **Reply To** address field and the polling address to populate the **From** address field. The internal name of this property is: `UseReplyToForReturnAddress`.

Configuration tab

The following configuration parameters are not presented on the ICEmail tab in Avaya IC Manager. Set these parameters on the **Configuration** tab.

Debug tab

The Debug tab does not include any IC Email server specific parameters.

Log Collector server

This section contains the following:

- General tab on page 488
- LogCollector tab on page 488
- Debug tab on page 488

Property	Recommended entry	Notes
OrigToCcInEDU	**0**: Original copy of the values in the To and CC fields is not maintained in EDU. **1**: If there is change in the values of the TO or CC fields, the Poller server creates new custom fields with the name, `XWF_OH_To` and `XWF_OH_Cc`. ICEmail server populates the corresponding new EDU fields, `currentemail.header.XWF_OH_To` and `currentemail.header.XWF_OH_Cc`, using values from the custom fields. **2**: Even if the Poller server does not add the custom fields `XWF_OH_To` and `XWF_OH_Cc` in email MIME, ICEmail server populates the corresponding new EDU fields, `currentemail.header.XWF_OH_To` and `currentemail.header.XWF_OH_Cc`, either using values from the custom fields or using the original values of the TO and CC fields when the original values are not changed. Default value is 0.	By default, the Poller server changes the values of the TO and CC fields of the incoming emails to address the loss of email addresses problem at IC agent side when an agent clicks the **Reply All** button. However, due to these changes, the system is unable to write the original values of TO and CC fields in EDU and EDU contains the changed values of TO and CC fields. You need to set the **OrigToCcInEDU** property to create a copy of To and CC fields in two new EDU fields. **Note:** ● You must restart the Email server after you configure the **OrigToCcInEDU** property. ● Email server uses the default value 0 if you did not configure the **OrigToCcInEDU** property. ● You must apply the **OrigToCcInEDU** property configuration to all the Email servers in the system so that all the Email server works in the same manner.

Property	Recommended entry	Notes
SearchFilterByTenant	1 The default value is 0.	While setting the `SearchFilterByTenant` property, ensure that you select **Couple** in the **CTI Type** field. The `SearchFilterByTenant` property name is case sensitive. After you set the `SearchFilterByTenant` property to 1, when an agent searches the emails, the search results contain only the emails for the tenant to which the agent belongs. If an agent or a supervisor is a member of more than one tenants, the search results display emails for all those tenants. Stop and start the Email server after you set the `SearchFilterByTenant` property. **Note:** If your migrated database version is earlier than IC release 7.1.5, you cannot use the `SearchFilterByTenant` property to restrict the email search on a particular tenant.
TerminateEDUDelay	7 The default value is 7 seconds.	This configuration is only applicable if the property Agent\Desktop\WrapupEnabled is set to false. This property introduces a delay between the time an email contact is wrapped and before its Eduid is terminated. Setting the parameter to a very low value might cause issues while creating Hub Eduids for email replies.
FromEmailExact	1 The default value is 0.	This is an optional configuration. If you want to search for messages where an exact match of the From address provided in the search query, configure FromEmailExact as 1. You must restart the Email server after you configure the FromEmailExact property.

General tab

Field	Recommended entry	Notes
Name	Email_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	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, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

LogCollector tab

The LogCollector server does not require any configuration. So, the LogCollector tab does not contain any fields that you need to configure for the LogCollector server.

Debug tab

The Debug tab does not include any LogCollector server specific parameters.

Java Application Bridge server

This server allows the Avaya Agent Web Client application to communicate with IC servers.

This section contains the following:

- General tab on page 489
- JavaAppBridge tab on page 490
- Debug tab on page 492

General tab

The following table describes the fields on the **General** tab:

Field	Recommended entry	Notes
Name	Enter a name for the Java Application Bridge. For example, JavaAppBridge_<Avaya Agent Web Client_*machine*>	Include the name of the system that hosts the Application server to identify the location of the JavaAppBridge.
Domain	Select an Avaya 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 Avaya 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 Avaya 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 For details, see *IC Installation Planning and Prerequisites*.
Host	Enter the IP address of the machine that hosts Avaya Agent Web Client.	
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 Avaya IC servers on the same system as Web Connector, Avaya recommends that you 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\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: `IC_INSTALL_DIR\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.

JavaAppBridge tab

The following table describes the fields on the **JavaAppBridge** tab:

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 when you configured an agent account for the Java Application Bridge. For example, enter dcobridge1.
IC Password	Enter the password of the agent account.	Use the password of the agent account that you created when you configured an agent account for the Java Application Bridge. For example, enter dcobridge1.

Field	Recommended entry	Notes
Agent List	No entry required.	Displays a list of the agents who are currently logged in to the Avaya Agent Web Client application server for this Java Application Bridge. To refresh the **Agent List**, close and re-open the Server Editor for the Java Application Bridge. You can also use the Agent List field to force the log out of an agent. **Note:** The list of agents displayed in **Agent List** does not include agents logged in to Avaya Agent or to Avaya Agent Web Client application servers that use a different Java Application Bridge.
Refresh Global Resources	Select this field after a supervisor creates or updates Global Resources.	The Java Application Bridge caches the global resources available for the associated application server. After a supervisor changes the available global resources, this field refreshes the cache and makes the changes to global resources available to the agents. To see the updated global resources, agents must log out and log in again. **Note:** If you do not refresh global resources, agents will not have access to the new or updated resources.
Refresh Email Templates	Select this field after a supervisor creates or updates email templates.	The Java Application Bridge caches email templates available for the associated application server. After a supervisor changes the available email templates, this field refreshes the email templates cache. To see the updated email templates, agents must log out and log in again. **Note:** If you do not refresh email templates, agents will not have access to the new or updated templates.

Field	Recommended entry	Notes
Refresh Address Book	After the supervisor creates, updates, or deletes an addressable agent or queue in IC Manager: 1. Click the **Ellipses (...)** button next to **Refresh Address Book**. 2. In the warning message that agents may experience slowdowns when you refresh the Address Book, click **Yes**. 3. In the message that advises the refresh has been successfully scheduled, click **OK**. IC Manager displays an alarm in **Alarm Monitor** to advise whether the refresh was successful.	The Java Application Bridge caches agent and queue information for the Address Book. After a supervisor changes one or more addressable agents or queues, this field refreshes the cache for the Address Book. For agents to see the changes in the Address Book, they must do one of the following: ● Refresh their Address Book views. ● Log out and log in again. **Note:** If you do not refresh the Address Book, agents will see updates to agents or queues in their Address Books.
Advanced Properties		
Supported Domains	Enter the domains, separated by a semicolon, this Java Application Bridge will support. An empty value means that all domains are supported.	Users not included in this semicolon separated list will be rejected.
Event Dispatcher Pool Size	Enter the pool size, in threads, of the event dispatcher queue. Default is 10.	Valid values are 1 to 1000.
Assign Thread Pool Minimum	Enter the minimum number of threads to allocate for assigning and deassigning. Default is 25.	Valid values are 10 to 2000.
Assign Thread Pool Maximum	Enter the maximum number of threads to allocate for assigning and deassigning. Default is 75.	Valid values are 10 to 2000.

Debug tab

The Debug tab does not include any Java Application Bridge server specific parameters.

License server

The License server ensures that Avaya IC can run the features and agents that have been purchased. This server also communicates with each of the Web License Managers in an Avaya IC system.

This section contains the following:

- General tab on page 493
- License Server tab on page 493
- Debug tab on page 494
- Advanced tab on page 495

General tab

Field	Recommended entry	Notes
Name	License_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya 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 machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

License Server tab

You can set the following parameters on the License tab (to view the advanced properties listed below, right-click and select Show Advanced Properties from the pop-up menu):

Field	Recommended entry	Notes
Warn about upcoming license expiry	Select this field.	
Alarm on no licenses	Select this field.	

Field	Recommended entry	Notes
WebLM Server URL	Enter the URL of the server page for a WebLM License Manager. **Note:** The URL for the WebLM is case-sensitive.	The default URL is `https://<machine_name>.<domain>:<webLM_port>/WebLM/LicenseServer` For example: `https://testbox.xyzcorp.com:8443/WebLM/LicenseServer` **Important:** Avaya recommends that you do not use the IP address of the machine in the URL. Note: For IC 7.3 and 7.3.1 the default WebLM port number was 8443. For IC 7.3.2 and later, the default WebLM port number is 52233.
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.

Debug tab

The Debug tab does not include any License server specific parameters.

Advanced tab

On this tab, you can view the license server status information by clicking the button next to **Server Status**. Following table explains about the important fields that displays the status of the licensing or working of Avaya IC:

Field	Mode	Notes
Mode of Operation	Normal Mode	License Server displays this mode when the WebLM is running with the correct license file and License server is is able to communicate with the WebLM. In this mode, License Server able to retrieve the licenses for both feature servers and the agents.
	Grace Mode	License Server displays this mode when the WebLM is not running, there is a network outage, or any other failure where the License server is not able to communicate with the WebLM. The License Server remains in this mode for 30 days. When License Server enters in this Mode, the new **Days Left of Grace** field appears in the server status list. If all the errors are rectified within the grace period of 30 days, Avaya IC shifts to the Normal Mode. In the Grace mode, Avaya IC operates as in the Normal mode.
	Restricted Mode	In this mode Avaya IC is restricted for performing operations. The feature servers and agents are unable to get licenses. Avaya IC becomes virtually nonfunctional. When the License server enters the Restricted mode, the Server Status list does not display the **Days Left of Grace** field.
Days Left of Grace		This field displays the number of days left as the grace period for updating the license files. The grace period starts from the 30 day and counts down to 1 day. Once the grace period becomes 0, the License server enters in the Restricted mode and the **Days Left of Grace** field is removed from the list.

Notification server

The Notification server provides scheduling and escalation rules, notifications, and report scheduling services to Avaya applications. It also provides access to other server-side communication services like fax, pager, email and printing. It can be used to fax documents through a server-based fax installation, eliminating the need for fax capability on each individual agent's machine. This reduces costs and administration expenses.

The Notification server polls the `qw_events` database table for events placed there by Avaya application clients. When Notification server finds an event marked for escalation, it verifies that the entry is valid and, if so, it starts the notification process. If the notification type is "Alert", the it places the event in the `qw_alert` database table. Avaya application clients poll the `qw_alert` table to pick up events stored there for them. For more information about polling, see Polling on page 499.

Note:
The Notification server does not encode email headers in a multi-lingual environment.

This section contains the following:

- General tab on page 496
- Notification tab on page 497
- Debug tab on page 499
- Polling on page 499

General tab

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

Notification tab

You can set the following parameters on the Notification tab to view the advanced properties listed below, right-click and select **Show Advanced Properties** from the pop-up menu:

Field	Recommended entry	Notes
IC Data Source	Select the data source for the application in the Avaya IC system.	If the Avaya IC system does not include any applications, select interaction_center.
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 and later.
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 and later.
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 desired.	The name of the work schedule the server should use to determine business time.

Field	Recommended entry	Notes
Notification Agent	Accept the default, or enter another agent number, if desired.	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	Check this field, if desired.	Select this option if the server should fire notifications.
Fire Escalations	Check this field, if desired.	Select this option if the server should send scheduled escalations.
Fire Scheduled Reports	Check this field, if desired.	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)
Advanced Properties		
Notification Script (Unix Only)	For Unix systems, enter the name of the script that the server should run when it sends a Notification.	Default: ../bin/qwscript.sh
Max Script Invocations (Unix Only)	For Unix systems, enter the maximum number of times the Notification script should be invoked.	Default: 20

Field	Recommended entry	Notes
Fax Address Format	Fax format to use when sending a fax. For details, see your fax application's software documentation.	Default: [FAX <fullname> / <faxnumber>]
FAX Mapi Profile (Windows only)	For Windows systems, enter the MAPI profile name that the Notification server should log into.	
Print Font (Windows only)	For Windows systems, the font name that will be used for printed messages. This string must match the font name as it is listed in the Windows font list. For example, you could enter Courier, Arial, or Times New Roman.	Default: Courier
Print Font SSize (Windows only)	For Windows systems, enter the size of the font to use for the printed message's subject line.	Default: 24
Print Font BSize (Windows only)	For Windows systems, enter the size of the font to use for the printed message's body text.	Default: 12
Interval to wait for DB reconnection	Enter the number of seconds the Notification server should wait before trying to reconnect to the database if the connection is lost.	Default: 300

Debug tab

The Debug tab does not include any Notification server specific parameters.

Polling

The Notification server handles events using both short and long polling.

For more details see:

- Short polling on page 500
- Long polling on page 500

Short polling

At regular intervals defined in the database table setup the `qw_events` table is polled to locate events with `state = new`. Those scheduled to initiate or trigger within the next 24 hours are scheduled internally and their `state` is changed to `scheduled`. Those items in the table not scheduled to trigger in the next 24 hours have their state changed to `future`. For each new `qw_events` record, invalidated `qw_events` records and their corresponding internally scheduled events are deleted. New records which are due to trigger after the next long poll have their `state` set to `future`.

Long polling

At regular intervals defined in the database table setup the `qw_events` table is polled to locate events with `state = future`. Those items scheduled within the next 24 hours are scheduled internally and their `state` changed to `scheduled`.

ORB server

The ORB server controls and maintains the IC servers on the system. Every machine on Avaya IC that runs servers must have an ORB server running on it. The ORB server starts, stops, and monitors the status of any server on its machine.

ORB servers on different machines communicate with each other to find the correct resource for a client request. If the requested server is not on the ORB server's machine, the request is routed to the correct ORB server on the other machine to handle the request. If a server is not yet started, the ORB server starts it.

For details, refer to *Core Services Programmer Guide*.

This section contains the following:

- General tab on page 501
- ORB tab on page 501
- Debug tab on page 501

General tab

Field	Recommended entry	Notes
Name	Enter a name for the ORB server. For example, ORBServer.	For all secondary ORB servers, include the domain in the server name to identify the server.
Domain	Select the Avaya 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 machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

ORB tab

Field	Recommended entry	Notes
Server Start Timer (sec)	Enter the number of seconds the ORB server should wait between attempts to start a server. Default is 15 seconds.	Use the minimum numbers of seconds that you want the server to wait.
Server Shutdown Timer (sec)	Enter the number of seconds the ORB server should wait for a server to shut down before moving on to shut down other servers. Default is 180 seconds.	Use the minimum numbers of seconds that you want the server to wait.

Debug tab

The Debug tab does not include any ORB server specific parameters.

Paging server

The Paging server serves as a communications bridge between Avaya Agent and the WebACD server. This server brokers messages to ensure they are sent to the correct agents and to the WebACD server.

Important:
When you create Avaya IC accounts for agents who handle chat contacts, make sure that the domain for those agents fails over to the domain that includes the Paging server.

This section contains the following:

- General tab on page 502
- Paging tab on page 503
- Debug tab on page 503

General tab

Field	Recommended entry	Notes
Name	Paging_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya 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 machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

Paging tab

Field	Recommended entry	Notes
Host Name	Enter the name of the system that hosts the Paging server.	For example, enter TESTBOX. Starting IC 7.3.3 and later, 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.
Service Port	4200	If you must change the default, see IC Installation and Configuration. Port conflicts can cause serious problems within the Avaya IC system.
ComHub Host Name	Enter the fully-qualified domain name of the machine that hosts the ComHub server.	For example, enter TESTBOX.xyzcorp.com.
Advanced Properties		
Comhub Port	Accept the default of 4001 or enter a new port number.	The service port for the ComHub server. If you must change this port, see 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. **Note:** If you change the default, you must also change this port for the WebACD server and the ComHub server.

Debug tab

The Debug tab does not include any Paging server specific parameters.

Poller server

The Poller server interacts with POP3, and IMAP4 servers to poll emails from the exchange server that you have configured. The Poller server stores the polled emails in the IC CCQ database.

This section contains the following:

- General tab on page 504
- Poller tab on page 504
- Configuration tab on page 509
- Debug tab on page 509

General tab

Field	Recommended entry	Notes
Name	Poller_<*domain*>	Include the domain in the server name to identify the server.
Domain	Avaya 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, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

Poller tab

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.

Field	Recommended entry	Notes
POP3 Cycle Wait Time (sec)	240	Specifies the default number of seconds that the server waits between checking for new contacts on a POP3 or IMAP4 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 or IMAP4 email server for the same email account. The maximum value that you can set for this field is 18000 seconds.
Advanced Properties		
Case Sensitive Email address validation	By Default, this check box is not selected. By default, the system compares the incoming email address in the **To** field with the Logon Account and polling account in a case in-sensitive manner.	If you set the value of this property to 1, the system compares the local-part of incoming email, which is the address from the **To** field, with the logon account and polling account configured in Avaya IC Manager in a case sensitive manner, as per RFC5321. The internal name of this property is: `EnableRFC5321LocalPart`. From IC 7.3.3 onwards this property does not enable case sensitive comparisons for email filters, but continues to be used internally. If a case sensitive comparison for email filters is required the regular expression should be provided accordingly. For more information see Creating email filters in IC Release 7.3.3 and later on page 124.
Populate Missing "From" header in incoming email	By Default, this check box is not selected.	Select this check box to handle the incoming emails that either do not have the value in the **From** field, or the value in the **From** field is invalid. The system sends the email replies to the email address in the **From** field of an incoming email. The functionality of this option is based on values that you set in the **Use "Reply-To"** and **Use "Sender"** properties.

Field	Recommended entry	Notes
Use "Reply-To"	By Default, this check box is not selected.	If you select the check box and if there is a valid **Reply-To** field in an email, the system copies the email address from the **Reply-To** field to the **From** field. You can view this field only when you select the **Populate Missing "From" header in incoming email** check box. This property takes higher priority over the `UseSenderIfNoFrom` property.
Use "Sender"	By Default, this check-box is not selected.	If you select this check box, the system uses the email addresses in the **Sender** field, if exists, to populate the empty or invalid **From** field. You can view this field only when you select the **Populate Missing "From" header in incoming email** check box. This property takes lower precedence to `UseReplyToIfNoFrom`.
Do Not Start new conversation thread, if Original email not found in DB	By Default, this check box is not selected. By Default, the system creates a new tracking, and treats such email as a new incoming contact.	If you select this check box and if the database does not have the copy of the original parent email of an incoming email, the system treats the incoming email as reply from the customer. The internal name of this property is: `NoNewTrackingIDForPurgedParent`.

Field	Recommended entry	Notes
Allow Only Emails with RFC compliant Email addresses	By Default, this check-box is selected. By Default, the system checks all the fields in an incoming email for RFC compliance and does not polls the email if the fields are not RFC compliant. **Note:** From IC 7.3.5 release and onwards, the behavior has changed. If an incoming email contains at least one RFC compliant header field (From or Sender or Reply-To), then such email would be processed by system. Otherwise the email will be bounced to bounced email address.	If you clear this check box, the system does not check the email addresses in the **From**, the **Reply-To**, and the **Sender** fields of an incoming email for RFC Compliance. However, the email is sent to the bounce email address configured in IC Manager for a particular email account. **Note:** If you do not want to send the email to the bounce email address, you must clear the **Allow Only RFC Compliant Emails to be processed** check box and specify the substitute email address in the **Substitute Email Address** field. The internal name of this property is: `DisableEmailAddressRFCCheck`. **Note:** From IC 7.3.5 release onwards, the behavior has changed. If you clear this check box, **Substitute Email Address** field would displayed. In case an incoming email does not contain any of the RFC compliant header fields (From or Sender or Replay-To) then the system uses email address entered in **Substitute Email Address** in the From field of incoming email.
Allow Only RFC Compliant Emails to be processed Note: From IC 7.3.5 release onwards this field is removed.	By Default, this check-box is selected. By Default, if all the header fields are missing, this email will be bounced to bounce email address.	If you clear this check box, the system does not treat the emails that arrives in the IC system without the **From**, the **Sender**, and the **Reply-To** fields, as SPAM and send that emails to an agent. You can view this field only when you clear the **Allow Only Emails with RFC compliant Email addresses** check box. The internal name of this property is: `DisableRFCCheckInSpamPlugin`.

Field	Recommended entry	Notes
Substitute Email Address	By default, the field is empty.	If you clear the **Allow Only RFC Compliant Emails to be processed** check box, you can enter the email address in the **Substitute Email Address** field, which the system uses in the **From** field of incoming email. If you do not enter any email address in the **Substitute Email Address** field, the system displays the bounce email address of the polling account in the **From** field. You can view the **Substitute Email Address** field only when the **Allow Only RFC Compliant Emails to be processed** check box is cleared. **Note:** From IC 7.3.5 release onwards, the behavior has changed. If you clear the **Allow Only Emails with RFC compliant Email addresses** check box, you can enter the email address in the Substitute Email Address field, which the system uses in the From field of incoming email. You can view the Substitute Email Address field only when the **Allow Only Emails with RFC compliant Email addresses** check box is cleared.
Allow emails with Only attachments	By Default, this check-box is not selected. By Default, the system treats an email with no body as a blank email and send that email to the customer as a bounce email.	If you select this check box, and if an incoming email body does not contain any text but contains an attached document, the system processes the email and does not treats that email as a blank email. The internal name of this property is: `BlankWithAttachment`.

Configuration tab

The following configuration parameters are not presented on the Poller tab in Avaya IC Manager. Set these parameters on the **Configuration** tab.

Property	Recommended entry	Notes
CCFieldPopulation	**0**: Poller server changes the email addresses in the **To** and **CC** fields. **1**: Poller server does not modify the values in the **To** and **CC** fields. Default value is 0 (Zero).	By default, the Poller server changes the **TO** and **CC** fields in MIME of all the incoming emails so that the **TO** field contains the IC polling address and all other addresses are moved to **CC** field. This displays only one email address in the **TO** field when an agent views the email. Also, when an agent click the **Reply All** button, all the non-polling addresses, that were moved to CC, are retained in the CC field of reply email. **Note:** ● You must restart the Poller server after you configure the **CCFieldPopulation** property. ● Poller server uses the default value 0 if you did not configure the **CCFieldPopulation** property. ● You must apply the **CCFieldPopulation** property configuration to all the Poller servers in the system so that all the Poller server works in the same manner.

Debug tab

The Debug tab does not include any Poller server specific parameters.

Report server

The Report server is used by the ADU server and the EDU server to record data unit (DU) information needed for historical reporting. When a data unit is terminated, it is passed to the Report server. The Report server may run mapping to convert the data unit into the appropriate format for reporting before it writes the information to the IC Repository.

This section contains the following:

- General tab on page 510
- Report tab on page 511
- Configuration tab on page 512
- Debug tab on page 513

General tab

Field	Recommended entry	Notes
Name	Report_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya 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 machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

Report tab

Field	Recommended entry	Notes
IC Data Source	Select the IC Data Source for the IC Repository database. Options are: ● ccq_contact ● repository ● interaction_center	If you used the default name, select `repository`.
Advanced Properties		
Focus	Enter the name of the Avaya application focus dedicated to creating reports. Default is `q_reportserver`.	
Request Handler Threads	Enter the number of threads in the request handler pool. Default is 10.	This is the number of threads that are able to handle requests simultaneously.
Database Writer Threads	Enter the number of threads that will write EDUs to the database. Default is 5.	
Child EDU to HUB Mapper Threads	Enter the number of threads that will update the HUB EDU from the child EDU when the Child EDU is retired. Default is 1.	

Field	Recommended entry	Notes
Saved File Reader Threads	Enter the number of threads that put EDUs back in queue from the file system when the database connection come up after being down. Default is 1.	This parameter is applicable only in Persistent mode. Persistent mode is enabled by checking the Enable Spooling field on this window.
Enable Spooling	Select this to place the Report server in Persistent mode. Default is checked.	A file named <eduid>.per is created per EDU termination in the `IC_INSTALL_DIR\etc\persist` directory. When the Report server writes the data from this EDU to the database, it deletes this file. If the Report server fails or the machine on which the Report server is inadvertently stopped, the persist (*.per) files help the Report server build its internal queue for EDUs. This ensures none of the EDUs are lost. It is recommended this check box always be checked.

Configuration tab

The following configuration parameters are not presented on the Report tab in Avaya IC Manager. Set these parameters on the Configuration tab.

Property	Description	Notes
retrycount	The number of additional attempts to process incoming requests in the event of a database error or a lost connection to an EDU server.	Value: integer Default: 0
archivetype	If this parameter is set to 1, then the Report server saves an incoming `Report.EventsIn` request to a temporary file called `temp\<EDUID>.tmp`.	Value: integer Default: 0

Debug tab

You can access the following Report server specific debug parameters on the Debug tab:

Field	Notes
Server Trace Level	Select a trace level from 0 to 10, where 0 is the lowest level of trace and 10 is the highest level. Trace messages are only written to the log if this parameter is set to 10.

Resource Manager server

The Resource Manager server is a Business Advocate server. You do not require this server for Avaya IC systems that do not include Business Advocate.

The Resource Manager server intelligently assigns contacts to available agents and maintains the universal queues for Business Advocate. The Resource Manager server is a Windows only server.

This section contains the following:

- General tab on page 513
- Resource Manager tab on page 514
- Configuration tab on page 514
- Debug tab on page 515

General tab

Field	Recommended entry	Notes
Name	ResourceManager_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	The Resource Manager server needs to be in a unique Avaya IC domain.
Host	Select the IP address of the machine from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

Resource Manager tab

This server does not have any advanced properties.

Field	Recommended entry	Notes
LRM	Select the name of the Logical Resource Manager for the Resource Manager from the LRM drop-down list.	A Logical Resource Manager can include one Resource Manager server, or a pair of Resource Manager servers where one is active and the other standby. If this server is one of a pair, use Business Advocate Component Manager to set the server role.

Configuration tab

The following configuration parameters are not presented on the Resource Manager tab in Avaya IC Manager. Set these parameters on the Configuration tab.

Property	Recommended entry	Notes
ChannelWeightFactorVoice	Assign a weight factor to the voice channel based on how the agents are configured to handle contacts. The weight factor determines the percentage of contacts routed to the voice channel.	Example, if two agents are configured to handle a total of two contacts, if agent max voice = 2, set this field to 2. This enables agents to handle 1 voice and 1 at a time.
ChannelWeightFactorChat	Assign a weight factor to the chat channel based on how the agents are configured to handle contacts. The weight factor determines the percentage of contacts routed to the chat channel.	If agent max chat = 1, set this field to 1. Agents can handle multiple chats and a time.
ChannelWeightFactorEmail	Assign a weight factor to the email channel based on how the agents are configured to handle contacts. The weight factor determines the percentage of contacts routed to email channel.	If agent max email = 1, set this field to 1. Agents can handle multiple emails at a time.

Debug tab

The Debug tab does not include any Resource Manager server specific parameters.

SiebelAED server

The Siebel AED server is only used when you integrate Siebel with Avaya IC. For details, see *Avaya IC for Siebel Integration Guide*.

SiebelAICD server

The Siebel AICD server is only used when you integrate Siebel with Avaya IC. For details, see *Avaya IC for Siebel 8 Integration*.

SiebelASIS server

The Siebel ASIS server is only used when you integrate Siebel with Avaya IC. For details, see *Avaya IC for Siebel 8 Integration*.

TS (Telephony) servers

The Telephony server (TS) is the Avaya server software responsible for linking Avaya IC to CTI products; such as private branch exchange (PBX) systems, automatic call distribution (ACD) systems, and interactive voice response (IVR) units.

Using the TS, other servers and clients in Avaya IC request telephony services (such as transfer or route a call, hang up a call) by invoking TS methods. These servers and clients also assign to the Avaya TS to receive telephone-related events.

You can configure the Telephony server to operate with the supported versions of the following switches.

- Avaya Communication Manager

For information about specific versions of these switches supported in the current release of Avaya IC, see *IC Installation Planning and Prerequisites*. For details, refer to the *IC Telephony Connectors Programmer Guide*.

This section contains the following:

- General tab on page 516
- TS tab on page 516
- TS tab for Avaya Communication Manager on page 517
- Configuration tab on page 522
- Hetero-switch tab on page 522
- Advocate tab on page 525
- Debug tab on page 525

General tab

The settings on this tab pertain to all of the supported switches.

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 Avaya 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 machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

TS tab

Use the following TS tab that corresponds to the switch for which you are configuring the Telephony server.

- TS tab for Avaya Communication Manager on page 517

TS tab for Avaya Communication Manager

The settings on this tab pertain to the versions of Avaya Communication Manager supported in the current release of Avaya IC.

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 will communicate.
ACD Model	Select Avaya Communication Manager	The model of the ACD that corresponds to the selected ACD Type.
ACD Protocol	Select asai	The protocol to be used between the TS and the ACD.
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 a name if it can be resolved into an IP) of the MAPD card set. Maximum length is 32.	The device through which the TS communicates with the ACD.
Signal Number	Specify a signal number when configuring multiple Avaya users on a single machine. There is no default value in the TS, but Avaya IC Manager sets this value to 1. Maximum length is 8.	The signal extension number of the ASAI line associated with each TS. The signal number is mandatory, if it is not specified, the TS will not be able to establish the link between users.
Call Control	Check to enable call control on every call.	If checked, enables the TS to monitor calls, not stations, on the system.
Advanced Properties		
Enable Call Containers	Check to create call containers for the TS. Default is checked.	If checked, the TS creates call containers to store information about the different legs of calls.

Field	Recommended entry	Notes
Enable Agent Containers	Check to turn on agent containers for the TS. Default is checked.	If checked, the ADU containers for the TS are turned on.
Use 5.6 State Fields	Check to give containers for agent states entries in the 5.6 style. Default is unchecked.	Example, ts.loginid. For details, refer to *IC Telephony Connectors Programmer Guide*.
Use 6.0 State Fields	Check to give containers for agent states entries in the 6.0 style. Default is checked.	Example, voice.loginid. For details, refer to *IC Telephony Connectors Programmer Guide*.
Wrap up by Client	Check to have the TS wait for the wrap-up process to be completed before removing the call information from memory. Default is unchecked.	If unchecked, the TS may remove the call information from memory before wrap-up is complete.
Wrap up Client Time to Live (min)	Enter the period of time, in minutes, that the TS waits for the wrap-up process to be completed by the client. Default is 15.	If unchecked, the TS issues a request for wrap up on behalf of the client.
Wrap up Server Time to Live (min)	Enter the period of time, in minutes, that the TS waits for the wrap-up process to be completed by the server. Default is 2.	If unchecked, the TS issues a request for wrap up on behalf of the server
Call Plan	Enter the number of digits on the external extension numbers used by the contact center. Default is 6.	This helps identify the call as internal to the switch.
Thread Pool Size	Enter the number of threads to allocate for the server thread pool. Default is 20.	
Queues Owned	Enter the name of the queue or queues for which the TS is responsible for creating queue ADUs.	The TSQS should not be associated with this queue in any way.
Default ANI	Enter the default ANI value, for incoming calls, which did not carry ANI information.	Add a space if you want to put an empty value instead of a default ANI value.

Field	Recommended entry	Notes
Suppress Logout Event	Check to ignore the logout event generated when the agent presses “Logout” on the hard phone. Default is unchecked.	This setting allows for Multiple Queue Assignment support because the agent can logout from the hard phone without terminating the softphone session. **IMPORTANT**: When this parameter is set to true, the TS also suppresses logout events that are caused by an agent logging out of the hardphone. In this case, the softphone and hardphone become out of sync.
Call Timeout	Enter the length of time, in seconds, to keep the call information in memory.	
Wait Time Before Merge Call (ms)	Enter the length of time, in milliseconds, to wait before sending a merge call.	• If the value of **Wait Time Before Merge Call** is less than 200 milliseconds, the Wait Time Before Merge Call value is below the operating range of 200 milliseconds. The value changes to 200 milliseconds. • If the value of **Wait Time Before Merge Call** is greater than 5000 milliseconds, **Wait Time Before Merge Call** value is above the operating range of 500 milliseconds. The value changes to 5000 milliseconds. **Note:** The delay before the call merge can be up to the maximum configured value and not necessarily the absolute configured value. If Communication Manager send events for the outbound call lag (except origination), the call merge happens immediately and does not wait further. For example, if the maximum value is configured for 5 seconds and in a call scenario, if and alert is received after 1 second for an outbound call leg, the merge happens immediately and does not wait for another 4 seconds. **Note:** This field is applicable only for Avaya Communication Manager Switch.
Route Timeout (sec)	Enter the length of time, in seconds, to keep route request information in memory.	

Field	Recommended entry	Notes
Wait Event During xfer	Clear the check box to merge the call after acknowledge (ACK) instead of waiting for an event during transfer/ conference.	
Abort on Link Down	Select the check box to abort (stop) the TS if the link goes down. Default is checked.	
Call Record Time to Live (hours)	Enter the maximum period of time, in hours, that a CtsCallRecord can remain in memory before the TS cleans it up. Default is 24.	A TpDisconnected event is generated for this record.
Enable Reason codes	Check to configure the ACD for reason codes. Default is unchecked.	The application can use reason codes for agent logouts and agent changeState to Busy.
Default Aux Reason Codes	Enter the code to use when the agent does not enter a code when changing their state to Busy. Default is 0.	This is only used if reason codes are enabled.
RONA Aux Reason Code	Enter the code to be used for RONA calls with Business Advocate. Default is 0.	The value in this field must match with the value in the `AuxRonaReasonCode` property in the **Agent\Desktop** properties section.
Dial by Equipment	Check to determine if the ACD requires the destination to be reached by equipment. Default is unchecked.	If you are using Avaya Business Advocate, do not check this field.
ACD Mode	Select the ACD mode that is compatible with the settings of the switch. Default is EAS.	This field must be set to EAS for the TS to support CVLAN Agent Events. If this field is set to ACD, the TS will not receive agent events.
ACD Version	Enter the version number of the switch software.	For example: Enter 6 for Avaya Communication Manager version 6.

Field	Recommended entry	Notes
RONA via Call Divert Request	Check to enable RONA (Redirect on No Answer). Default is checked.	This tells the TS that the switch is capable of handling a call deflection (divert) on an alerting device or if the call needs to be answered before it can be transferred or conferenced to another destination.
RONA indicated via Call Divert	Check to enable the switch to send a divert event when RONA is in progress.	
Ccti Trace Level	Select the desired log level for Ccti. Default is info.	Valid values are debug, info, warning, and error.
Cpbx Trace Level	Select the desired log level for Cpbx. Default is info.	Valid values are debug, info, warning, and error.
TsV5 Trace Level	Select the desired log level for TSV5. Default is info.	Valid values are debug, info, warning, and error.
DTMF Tone Duration	Enter the duration length of each DTMF tone between 6 and 35. Default is 35.	This value specifies the length of each DTMF tone in 0.01 second increments. If you enter 35, the tone duration length 0.35 is applied at the switch. If this value is set out of the 6 to 35 range, the default value of 35 is set automatically.
DTMF Pause Duration	Enter the duration length of each DTMF pause between 4 and 10. Default is 10.	This value specifies the length of the pause between tones in 0.01 second increments. If you enter 10, the pause duration length 0.01 is applied at the switch. If this value is set out of the 4 to 10 range, the default value of 10 is set automatically.
Cutthrough Waittime	Enter the number of seconds the TS will wait for an event after it receives a C_CUT_THROUGH event. Once this time expires, the TS assumes the call has been answered.	Values: 0 - 30 (seconds).

Configuration tab

The following configuration parameters are not presented on the TS tab in Avaya IC Manager. Set these parameters on the Configuration tab:

Property	Recommended entry	Notes
allow_names_mixed_case	Enter "true" to enable processing of queue names in the case that comes in. If set to "false", queue names will be set to lower case.	Values: true or false.
blockedani	Enter the ANI number you want to display if the ANI currently displays as ***** because the caller has caller ID blocked.	If an ANI is not present, translates to the default ANI specified in the Default ANI parameter. If the ANI is ***** or #####, translates to this value.
cutthrough_waittime	Enter the number of seconds the TS will wait for an event after it receives a C_CUT_THROUGH event. Once this time expires, the TS assumes the call has been answered.	Values: 0 - 30 (seconds).

Hetero-switch tab

The settings on this tab pertain to all of the supported switches.

Field	Recommended entry	Notes
Enable Hetero Switch Transfer	Check to enable the Multi Site Heterogeneous Switch feature. Default is unchecked.	Checking this parameter displays the other parameters listed in this table.
Default Route Point	Enter the default destination for route point calls received to which the ANI does not match.	
ANI Validation	Check to indicate the ANI should be validated when the TS receives call in a reserved DN. Default is unchecked.	

Field	Recommended entry	Notes
Queue Time to Live (hr)	Enter the period of time, in hours, an entry for a queue that is supported by another TS should stay in the queue. Default is 24.	
Hetero Lifetime (sec)	Enter the period of time, in seconds, that reserved DNs should reside in the Locked state. Default is 5.	
Use DNIS	Check to have the TS use DNIS resolution when a call arrives at a reserved route point. Default is unchecked.	
Use Local ANI	Check to have the TS check the Local ANI parameter prior to routing the call. Default is checked.	
TS Group	Enter the name of the group to which this TS is assigned.	TS groups are defined on the Avaya IC Manager Configuration tab.
Reserved DN Table	Enter the reserved DNs that will be used for hetero switching.	
Multiple ANI Table	Enter the s of the ANIs that will be used for hetero switching.	
Dial Translation Table	Specifies the translation rules for PSTN number translation rules.	Used for speed dialing.

Field	Recommended entry	Notes
Advanced Properties		
Transfer Resolution Table	Specifies the parameters for transfer resolution between Telephony servers	Multiple lines of four fields that contain: ● Alias (or UUID) of the destination TS to which this rule applies. ● Value indicating if the connection to this TS supports Take Back and Transfer. ● Value indicating if connection to the destination TS can be done using ISDN UUI. ● Sequence of numbers to be prepended to the device number in the ADU that are used to reach the destination TS.
Take Back and Transfer Sequence	Specifies the sequence to transmit to activate Take Back and Transfer.	
Take Back Transfer Type	Specifies the type of Take Back and Transfer to be implemented. Default is inband.	
Trunk to Trunk Transfer Enabled	Check to enable trunk to trunk transfer for the switch and the TS.	

Advocate tab

The settings on this tab pertain to all of the supported switches.

Field	Recommended entry	Notes
Enable Advocate	Check to enable the optional Avaya Business Advocate feature. Default is unchecked.	Checking this parameter displays the other parameters listed in this table.
Default RONA Destination	Select the ID of the wait treatment to route a call that is not answered.	RONA (Redirect on No Answer) is used to re-route a call that was not answered by the agent to whom it was originally sent. The TS sends the call to a wait treatment queue where the Resource Manager finds another agent for the call. The wait treatment queue ID is created in the Device Manager of Avaya IC Manager. This setting is required on every TS that hosts Advocate agents and does not have an associated TSA server in its IC domain. This setting is not required for TSes that handle incoming call processing and are not associated with any link group.
Optional Backup Link for Advocate	Select the link to you as a backup in the event the primary CTI link goes down.	

Debug tab

The Debug tab does not include any Telephony server specific parameters.

Telephony Queue Statistic servers

The Telephony Queue Statistics server (TSQS) is the Avaya IC server that monitors the voice channel and maintains queue statistics in the Agent Data Unit (ADU) server. When running On the Avaya Communication Manager switch, the TSQS relies on the Avaya TS to interact with the switch.

The TSQS can be configured to operate with Avaya Communication Manager.

For information about specific versions of these switches supported in the current release of Avaya IC, see *IC Installation Planning and Prerequisites*. For details, refer to *IC Telephony Connectors Programmer Guide*.

This section contains the following:

- General tab on page 526
- Debug tab on page 526
- TSQS tab on page 527

General tab

Field	Recommended entry	Notes
Name	TsQueueStatistics_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya 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 machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

Debug tab

The Debug tab does not include any Telephony Queue Statistics server specific parameters.

TSQS tab

Use the following TSQS tab that corresponds to the switch for which you are configuring the TSQS.

- TSQS tab for Avaya Communication Manager on page 527

TSQS tab for Avaya Communication Manager

The settings on this tab pertain to the versions of Avaya Communication Manager supported in the current release of Avaya IC.

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.
ACD Model	Displays Communication Manager 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 used by your TS configured for Avaya switch.
Advanced Properties		
Update Interval (secs)	Enter the number of seconds between updates to the ADU server with queue statistics. Default is 10 seconds.	
Oldest ADU Timestamp	Select this to enable backward compatibility to eContact 5.6. Default is unchecked.	Lets the TSQS keep the oldest field in the ADU as the length of time (in seconds) that the oldest call is in queue. The default uses the timestamp of when the oldest call arrived.

Field	Recommended entry	Notes
Forced ADU Update	Check to enable the server to issue an ADU.SetValues command even if none of the parameter values changed. Default is unchecked.	
Maximum Calls per Queue	Enter the maximum number of calls to track in a single queue. Default is 4,096	

TSA (Telephony Services Adaptor) server

The Telephony Services Adaptor (TSA) server is a Business Advocate adaptor for the Telephony server. The TSA server manages server interactions for Business Advocate that are required for voice contacts. Business Advocate requires a TSA server for every switch in your Avaya IC system.

This section contains the following:

- General tab on page 528
- TSA tab on page 530
- Debug tab on page 531

General tab

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

Field	Recommended entry	Notes
Domain	Select the Avaya IC domain for the server from the drop-down list.	The TSA server must be in the same domain as the Telephony server that the TSA server services. For example, select `Voice1` from the drop-down list if the Telephony server is in the Voice1 domain.
Host	Select the IP address of the machine from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

TSA tab

This server does not have any advanced properties.

Field	Recommended entry	Notes
LRM	Click the **Ellipsis (…)** button, and in the LRM dialog box: ● Click the **New** button. ● Select a Logical Resource Manager from the drop-down list. ● Repeat these steps for each Logical Resource Manager that you want the TSA server to manage. ● Click **OK**.	Assign at least one Logical Resource Manager to each TSA server. You can assign multiple Logical Resource Managers to a TSA server. **Note:** For a complete description of this field, see *IC Business Advocate Configuration and Administration*.
Contact Handling	Click the **Ellipsis (…)** button, and in the Contact Handling dialog box: ● Click the **New** button. ● In the **Destination** field, enter a DN that you want the TSA server to monitor or use the default. ● Accept the default **Qualification Flow** or enter a custom workflow that sets qualifiers for voice contacts. ● Accept the default **Exception Flow** or enter the routing exception workflow for the TSA to use for voice contacts. ● Click **OK**.	If you select default, the TSA server handle all contacts to the Telephony server that have not been specifically assigned with a Destination DN. If the TSA server monitors a backup CTI link as well as a primary link, include the destination DN of the backup link when you set up contact handling. The default qualification workflow is `advocate.qualifyvoice_adv`. The default workflow is the sample routing exception workflow, advocate.handle_exception. For a custom workflow, enter `<workflow_project>.<workflow>` This field is case-sensitive. Use all lower case letters.
Transfer Exception Flow	Accept the default or enter a custom workflow to handle exceptions for transferred voice contacts.	The default workflow is the sample routing exception workflow, advocate.handle_exception. For a custom workflow, enter *<workflow_project>.<workflow>* This field is case-sensitive. Use all lower case letters.

Field	Recommended entry	Notes
Enable Sip for TSA	Select this check box.	
Buddy TSA	Select the buddy TSA from the drop-down list.	

Debug tab

The Debug tab does not include any TSA server specific parameters.

VOX server

The VOX server is the connector used by Interactive Voice Response units (IVRs) to communicate with the Avaya Telephony server. The VOX server sends and receives messages from both environments.

Note:
VOX server is compliant with the `E.164` based dial plan.

For details, refer to *VOX Server Programmer Guide*.

This section contains the following:

- General tab on page 532
- VOX tab on page 532
- VRU tab on page 538
- Configuration tab on page 539
- Debug tab on page 539

General tab

Field	Recommended entry	Notes
Name	VOX_<*domain*>_<*IVR*>	Include the name of the domain and the IVR in the server name to identify the server.
Domain	Select the Avaya 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 machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

VOX tab

Field	Recommended entry	Notes
Workflow Server	Select the Workflow server for IVR contacts.	The Workflow server that you created for the VOX server.
Maximum Wait Time	Enter the maximum number of seconds the VOX server waits for a connection to an IVR. This value needs to be greater than the value of Disable wait. Default is 8.	If an attempt by the VOX server to connect to an IVR takes more seconds than the value set here, the attempt is aborted. Since connect attempts are done synchronously, you should set this parameter for IVRs that tend to become available and unavailable frequently. If this parameter is set to 0 (the default), the VOX server will try until a system-defined limit is reached. **Note:** This parameter has no effect if the IVR is of the kind that connects to the VOX server.

Field	Recommended entry	Notes
Disable Wait	If an attempt by the VOX Server to connect to an IVR fails, and the failed attempt took more than the maximum number of seconds in this field, the VOX server disables all future attempts to connect to that IVR. This value needs to be less than the value of Maximum Wait Time. Default is 6.	If the VOX server disconnects from the IVR, stop and restart the VOX server to reconnect to the IVR.
VOX Listener Port	Enter the port number of the VOX server expected to listen for the VRU to connect. Port 3000 is recommended. Default is 0, disables the listener.	If you must change this port, see IC Installation and Configuration for a list of the default port numbers used by the other Avaya IC servers. Port conflicts and cause serious problems within the Avaya IC system.
Show Pings	Select the check box to include pings in the log. By default, the check box is not selected.	
Wait for New Call	Enter the time (in seconds) that the VOX server will wait for VOX.newcall after it receives a TS.IncomingCall.event. Default is 10.	If the designated time expires, the VOX server raises an alarm (*Late*) and ignores the TS.IncomingCall.event. If set to 0, the VOX server waits until a system-defined limit is reached.

Field	Recommended entry	Notes
Wait After Disc.	Enter the time (in seconds) that the VOX server will wait for VOX.newcall after receiving a TS.Disconnect.event. Default is 1. 0 seconds is an acceptable value.	If the designated time expires, the VOX server raises an alarm (*Abandon*) and ignores the TS.Disconnect.event. This parameter will never cause the VOX server to wait longer than the Wait For New Call parameter would allow. In general, a TS.Disconnect message that precedes a VOX.newcall should indicate that the call did not arrive at the VRU. No VOX.newcall will ever be received for that call. However, a delay in processing might cause a VOX.newcall to be emitted a few seconds late; so the VOX.newcall for a call and the TS.Disconnect that ends it can "cross". (On a system, VRU, or network that is heavily loaded—and VRU messages are subject to delays from all three—messages can be delayed by 2 seconds or more.) This parameter helps prevent misassociations from occurring if the TS.Disconnect precedes the VOX.newcall with which it should be associated. The logic is that a VOX.newcall, produced by the same telephone call that produced the TS.Disconnect, should still arrive significantly faster than a VOX.newcall that was produced by a second call coming in after an aborted call. Therefore, if an appropriate maximum time is chosen, there should be no misassociation of an aborted call's TS.Disconnect with a second call's VOX.newcall.
Wait For Incoming Call	Enter the time (in seconds) that the VOX server will wait for TS.IncomingCall.event after receiving a VOX.newcall request. Default is 8.	If the designated time expires, the VOX server raises an alarm (*Late*) and ignores the VOX.newcall request. If set to `0`, the VOX server waits until a system-defined limit is reached.

Field	Recommended entry	Notes
AssignOK	Clear this check box to turn the AssignOK informational alarm off. Default is selected.	
Wait for Connect	Turns off/on the requirement that the VOX server wait for a TS.Connect.event before proceeding with call handling. Default is checked.	If checked (on), a TS.IncomingCall.event must be followed by a TS.Connect.event before the VOX server will proceed with call handling. If the VOX server does not get a TS.Connect.event, a second TS.IncomingCall.event will cause it to abandon the first call (raising the alarm *NoDeliver*) and take up the second. If unchecked (off), whenever the VOX server receives a TS.IncomingCall.event, it pretends that it has seen a following TS.Connect.event and does not wait. This is not recommended.
Scripter Method		
Debug Output	Enter a filename to initialize a special debugging facility.	The debugging facility places its output in the file indicated. This output is an analysis of most of the traffic between the IVRs and the VOX server, and describes each call received.
Incoming/NewCall range (sec)	Enter the number of seconds that may pass between a TS.IncomingCall.event from the Telephony Server and the VOX.newcall from the IVR, before the debug code assumes that something is wrong. Maximum is 15. Default is 0 (disables this check).	Used with the Debug Output parameter. This parameter has no effect on the Wait For New Call parameter.

Field	Recommended entry	Notes
Connect/NewCall range (sec)	Enter the number of seconds that may pass between a TS.Connect.event from the Telephony Server and the VOX.newcall from the IVR, before the debug code assumes that something is wrong. Maximum is 10. Default is 0 (disables this check).	Used with the Debug Output parameter. This parameter has no effect on the Wait For New Call parameter.
Disconnect/Gone range (sec)	Enter the number of seconds that may pass between a TS.Disconnect.event from the Telephony Server and the VOX.gone from the IVR, before the debug code assumes that something is wrong. Maximum is 45. Default is 0 (disables this check).	Used with the Debug Output parameter. This parameter has no effect on the Wait For New Call parameter.
No Telephony Server	If selected, informs the VOX server there is no Telephony Server available. By default, the check box is not selected.	If checked, this causes the VOX server to issue a VDU.Create request upon receipt of a VOX.newcall command. Otherwise it is the Telephony Server's responsibility to request the creation of an EDU. (The usual reason that no Telephony Server is available is because a network VRU is being used, or because no PBX is being used.) In the unusual case where some lines are controlled by a TS and some are not, *do not check this parameter*. Instead, use the exclamation point (!) in association with the relevant Extensions parameter values.

Field	Recommended entry	Notes
pseudo-ANIs	Used only with network IVRs. A comma-separated list of pseudo-ANIs that can be used when transferring calls.	The size of this list determines the maximum number of transfers involving a network IVR that can be in progress at any give time. Elements in the list may have one of the following four forms: ● 6175551212 - The single value 6175551212 ● 61755512XX - The one hundred values 6175551200 through 6175551299 ● 6175551200-6175551299 - The one hundred values 6175551200 through 6175551299 ● 6175551200-99 - The one hundred values 6175551200 through 6175551299 A list containing the elements: 6175551208,6175551209,61755512 1X,6175551220-4 would assign all the numbers 6175551208 through 6175551224 to be available as pseudo-ANIs. If more than one VOX server is being used, each VOX server must have a unique list of pseudo-ANIs.
pseudo-ANI Timeout (sec)	Used only with network IVRs. The time (in seconds) that the VOX server waits before breaking the association between a pseudo-ANI and an EDU. Default is 20. Minimum 10.	When a network VRU is ready to transfer a call, it issues a VOX.pseudo_ani request to the VOX server with the EDUID of the call for which it wants the pseudo-ANI. The VOX server responds with a pseudo-ANI and preserves an association between the supplied pseudo-ANI and the provided EDUID, for no longer than the time specified by this parameter.
Enable Extended Data Support	By default, the check box is not selected.	If you select the check box for this field, VOX server extracts the extended UUI data from the `TS.IncomingCall` event and sends that data while transferring the call using TS.TransferEx method. If you do not select the check box, the HttpVOX server calls the `TS.TransferEX` method with **NULL** as the extended data.

VRU tab

Press the **New vru** button to display the following fields on the **VRU Editor** dialog.

Field	Recommended entry	Notes
VRU System Name	Enter the IP address of the IVR.	You must have defined a mapping between the network name of the IVR and the IP address of the IVR.
TCP/IP Port	Enter the Port through which the VOX server connects to the IVR. If the IVR connects directly to the VOX Server, leave this field empty. Default is 3000.	Port 3000 is the port that the CONVERSANT® System for Interactive Voice Response uses. If the IVR connects directly to the VOX Server, enter the VOX Listener Port on the VOX tab. If the IVR listens for a connection from the VOX Server, enter 0 in this field, then go to the VOX tab and enter the listener port in the VOX Listener Port field. If your system supports named ports ("services"), you can enter the service name. The service name must not start with a digit.
Initiate connection to VOX	Select this field if the IVR connects directly to the VOX server. By default, the check box is not selected.	
Ping Time	Enter the expected time (in seconds) between pings for the IVR.	This parameter is displayed when the "Initiate connection to VOX" setting is selected. Leave this field blank to disable this parameter. If the IVR does not issue pings at least this quickly, Avaya IC issues alarms.

Press the **New Line** button to display the following fields on the **VRU Line Editor** dialog.

Field	Recommended entry	Notes
VRU	Displays the IP address of the IVR that you entered at the VRU Editor tab.	Avaya IC Manager completes this field with the IVR system name.
Extensions	Enter the telephone line extension number to associate with the Channel number.	If the line numbers are sequential, you can associate multiple phone and channel numbers in a single entry. For example, enter: `4100-4104` in this field and 0 in the Channel field to associate extension 4100 with channel 0, 4101 with channel 1. If the line numbers have leading zeros, a range preserves the zeros only if all line numbers in the range have the same number of digits.
Channel	Enter the Channel number that the IVR uses to recognize the line number in the Extension field.	

Configuration tab

The following configuration parameter is not presented on the VOX tab in Avaya IC Manager. Set this parameter on the Configuration tab:

Property	Recommended entry	Notes
complete_timeout_alarm	When set to true, sends an alarm when the ANI used to transfer the call is being reused without knowing if the call reached its destination. Default is true.	Values: true - false.

Debug tab

The Debug tab does not include any VOX server specific parameters.

WAA (Web Advocate Adaptor) server

The Web Advocate Adaptor (WAA) server is the Business Advocate adapter for the WebACD server. The WAA server manages server interactions for Business Advocate that are required for chat contacts and email contacts.

Note:

The WAA server adds **sc.state** and **sc.qat** fields in the EDU of a contact. The values of these fields does not have any reference outside the WAA server.

Do not use the **sc.qat** and **sc.state** fields. The values in these fields are used only for the internal purpose.

This section contains the following:

- General tab on page 540
- WAA tab on page 541
- Debug tab on page 542

General tab

Field	Recommended entry	Notes
Name	WAA_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	The WAA server must be in the same Avaya IC domain as the WebACD server. For example, select `Web` from the drop-down list if the server is in the Web domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

WAA tab

You must select the **Configure Advocate for Email Channel** and **Configure Advocate for Chat Channel** fields to view the other fields on the WAA tab.

Field	Recommended entry	Notes
Configure Advocate for Email Channel	Select this check box if you want Business Advocate to route email contacts.	After you select the check box, Avaya IC Manager displays the remaining fields required to configure the email channel.
Email LRM	Select a Logical Resource Manager from the drop-down list.	This is the Logical Resource Manager that the Web Advocate Adaptor server will communicate with for email contacts.
Email qualification Flow	Accept the default workflow or enter a custom workflow for the WAA server to use to route email contacts.	The default is the sample email qualification workflow, advocate.qualifyemail_advocate. To use a custom workflow, enter <*workflow_project*>.<*workflow*> This field is case-sensitive. Use all lower case letters.
Email Routing Exception Flow	Accept the default workflow or enter a custom workflow for the WAA server to use for email contacts.	The default is the sample email routing exception workflow, advocate.route_exception. To use a custom workflow, enter <*workflow_project*>.<*workflow*> This field is case-sensitive. Use all lower case letters.
Email Transfer Exception Flow	Accept the default transfer exception workflow or enter a custom workflow for the WAA server to use for email contacts.	The default is the sample transfer exception workflow, advocate.route_exception. To use a custom workflow, enter <*workflow_project*>.<*workflow*> This field is case-sensitive. Use all lower case letters.
Configure Advocate for Chat Channel	Select this check box if you want Business Advocate to route chat contacts.	After you select the check box, Avaya IC Manager displays the remaining fields required to configure the chat channel.
Chat LRM	Select the Logical Resource Manager that handles chat contacts.	This is the Logical Resource Manager that the Web Advocate Adaptor server will communicate with for chat contacts.

Field	Recommended entry	Notes
Chat Qualification Flow	Accept the default workflow or enter a custom workflow for the WAA server to use to route chat contacts.	The default is the sample chat qualification workflow, advocate.qualifychat_adv. For a custom workflow, enter <*workflow_project*>.<*workflow*> This field is case-sensitive. Use all lower case letters.
Chat Routing Exception Flow	Accept the default workflow or enter a custom workflow for the WAA server to use for chat contacts.	The default is the sample chat routing exception workflow, advocate.route_exception. For a custom workflow, enter <*workflow_project*>.<*workflow*> This field is case-sensitive. Use all lower case letters.
Chat Transfer Exception Flow	Accept the default workflow or enter a custom workflow for the WAA server to use for chat contacts.	The default is the sample transfer exception workflow, advocate.route_exception. For a custom workflow, enter <*workflow_project*>.<*workflow*> This field is case-sensitive. Use all lower case letters.
Advanced Properties		
Default WACD Cluster	Default WebACD cluster name configured.	

Debug tab

The Debug tab does not include any WAA server specific parameters.

WebACD server

The WebACD server is the call distributor for chats and emails. This server is responsible for assigning tasks to agents and tracking the different states such interactions undergo. It makes use of the Attribute, Paging, Email and Comhub servers to complete support operations such as managing agent logon/logout states and the actual administration of the interactions.

Note:
For an invalid email qualification, WACD Administration page displays the message *Waiting for qualification*. The invalid qualification means, the Workflow to qualify a chat or an email is not available, or taking more time to qualify and WACD times out.

This section contains the following:

- General tab on page 543
- WACD tab on page 543
- Advocate tab on page 547
- Configuration tab on page 547
- Debug tab on page 550

General tab

Field	Recommended entry	Notes
Name	WebACD_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	For example, select `Web` from the drop-down list.
Host	Enter or select the machine's IP address from the drop-down list.	When you select the host, Avaya IC Manager fills in Directory, Port, and Executable.

WACD tab

This server does not have any advanced properties.

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.

Field	Recommended entry	Notes
Service Port	Default is 4010	If you must change this port, see 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	Default is `interaction_center`	
WACD Webserver	Enter the name and domain of the system that hosts the Web Administration pages.	For example, enter TEXTBOX.xyzcorp.com.
Port	Enter the port that the WebACD server uses for connections with Web applications. Default is 80.	Default port is 80 unless you plan to configure SSL for your website. If you must change this port, see 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.
Protocol	Select the protocol that you use to connect to the Website.	Select **`http`** unless you plan to configure SSL for your Website. For details on SSL, see 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 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)	Default is 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 will wait 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.
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 will write summaries at 12:00, 12:05, 12:10, etc.

Field	Recommended entry	Notes
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	Select the email cluster name.	This is the default email cluster to which agents connect after logging in to the IC agent application. If you want to use the email channel, you must configure the default email cluster. If you do not configure this default email cluster, agents can use email functionality. The default email cluster contains two Email servers that acts as redundant Email servers to each other. **Important:** If you do not set the Default Email Cluster field, the Email Account panel does not display the template data.
Advanced Properties		
Reset Script Iteration	By Default, this check box is selected.	If this check box is selected, the queue scripts starts from iteration zero, which means the priorities of the tasks are reset to zero, if you restart the WACD server. If the check box is not selected, WACD recreates the tasks at the same priority and workgroup that it had prior to the restart. The internal name of this property is `ResetScriptIteration`. This property is used only for email contacts.
Number of re-tries to send the RequestResource to WAA	1000	This property controls the number of `WACD.RequestResource` requests that WACD Server makes to WAA server. This property is used only for chat contacts in the Advocate mode. The internal name of this property is `RequestResourceRetryCount`.

Advocate tab

This tab does not have any advanced properties.

Field	Recommended entry	Notes
Enable Advocate	*No recommended entry*	Select this check box to use Advocate to route calls within your Avaya IC system.

Configuration tab

This tab allows you to enter additional configuration parameters for the WebACD server, including the following configuration parameters:

- emailservername on page 547
- ewtFlavor on page 548
- ewtAhtSeed on page 548
- ronaenqueueworkgroup_chat on page 549
- ronaenqueueworkgroup_email on page 549

emailservername: If you install the IC Email server on a different system from the WebACD server, you need to enter the emailservername configuration parameter for the WebACD server. To do so:

1. In Avaya IC Manager click the **Server** tab.
2. In the right pane, double-click the WebACD server to edit the properties.
3. In the **Server Editor** dialog box, click the **Configuration** tab.
4. Click **New**.
5. Enter:
   - Name - `emailservername`
   - Value - *`<IC Email system name>`*

   where the name must be `emailservername` (all lowercase) and the value is the name of the system on which the IC Email server is running.
6. Click **Ok**.

ewtFlavor: If you want to present Estimated Wait Time (EWT) in case of a non-Business Advocate (BA) chat, enter the ewtFlavor configuration parameter for the WebACD server. This parameter has three possible values, as described in the following table:

Value	Description
0	EWT is off. This is the default value.
1	Exact. Avaya IC 7.3.5 does not support Exact.
2	Optimized

To configure the ewtFlavor parameter, do the following:

1. In Avaya IC Manager click the **Server** tab.
2. In the right pane, double-click the WebACD server to edit the properties.
3. In the **Server Editor** dialog box, click the **Configuration** tab.
4. Click **New**.
5. Type:
   - Name - `ewtFlavor`
   - Value - *2*

   `ewtFlavor` supports only the value of 2. EWT(Optimized) provides the far end estimate.
6. Click **Ok**.

   You must restart the WACD server after you configure the ewtFlavor parameter.

ewtAhtSeed: If you want to configure the start "seed" value for Agent Average Handling Time (AHT). Handle time is the time from when an agent accepts a task till the time the agent wraps up the task. An updated average handle time for agents is maintained on WACD as agents complete their tasks.

To configure the ewtAhtSeed parameter, do the following:

1. In Avaya IC Manager click the **Server** tab.
2. In the right pane, double-click the WebACD server to edit the properties.
3. In the **Server Editor** dialog box, click the **Configuration** tab.
4. Click **New**.
5. Type:
   - Name - `ewtAhtSeed`
   - Value - *<start seed value for AHT>*

   The value of `ewtAhtSeed` is set in seconds and by default it is set to 60. `ewtAhtSeed` value is used to calculate EWT for the first time on every WACD restart.

6. Click **Ok**.

   You must restart the WACD server after you configure the ewtAhtSeed parameter.

ronaenqueueworkgroup_chat: If you want to override the default behavior of the WebACD server when a chat contact enters RONA, enter the ronaenqueueworkgroup_chat configuration parameter for the WebACD server. This parameter has two possible values, as described in the following table:

Value	Description
0	The WebACD server will not add a chat contact to the queue for the agent's workgroup upon RONA.
1	The WebACD server will add a chat contact to the queue for the agent's workgroup upon RONA. This is the default behavior for RONA. You do not need to add this parameter to use this setting.

To use the ronaenqueueworkgroup_chat parameter to change the default RONA behavior:

1. In Avaya IC Manager click the **Server** tab.
2. In the right pane, double-click the WebACD server to edit the properties.
3. In the **Server Editor** dialog box, click the **Configuration** tab.
4. Click **New**.
5. Enter:
   - Name - `ronaenqueueworkgroup_chat`
   - Value - `0`
6. Click **Ok**.

ronaenqueueworkgroup_email: If you want to override the default behavior of the WebACD server when an email contact enters RONA, enter the ronaenqueueworkgroup_email configuration parameter for the WebACD server. This parameter has two possible values, as described in the following table:

Value	Description
0	The WebACD server will not add an email contact to the queue for the agent's workgroup upon RONA.
1	The WebACD server will add an email contact to the queue for the agent's workgroup upon RONA. This is the default behavior for RONA. You do not need to add this parameter to use this setting.

To use the ronaenqueueworkgroup_email parameter to change the default RONA behavior:

1. In Avaya IC Manager's **Server** tab, double-click on your WebACD server so that you can edit its properties.
2. In the Server Editor dialog box, select the **Configuration** tab.
3. Select **New**.
4. Enter:
   - Name - `ronaenqueueworkgroup_email`
   - Value - `0`
5. Select **OK**.

Debug tab

You can access the following WebACD server specific debug parameters on the Debug tab:

Field	Notes
Log Trace Level	Logs WebACD server events. Select a trace level from 10 to 100000, where 10 is the lowest level of trace and 100000 is the highest.

Web Scheduled Callback server

The Web Scheduled Callback server retrieves the scheduled call from the database and delivers that scheduled call to an agent as a Chat & Callback task.

The Web Scheduled Callback server is also responsible for the following tasks:

- Establishing a connection with the repository database
- Polling the database at regular intervals to find the scheduled call
- Creating a Chat&Callback task at a scheduled time

Web Scheduled Callback server is a lightweight server. Therefore, the callback load on the Web Scheduled Callback server depends on the call queue size, call timeout interval, and schedule interval.

The maximum callback load also depends on the number of agents logged in to the Avaya IC system at a time, and the chat task load of an agent. There is no any specific formula to calculate the scheduled callback load.

This section contains the following:

- General tab on page 551

- WSCallback tab on page 551
- Debug tab on page 553

General tab

Field	Recommended entry	Notes
Name	WSCallback_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya IC domain for the server from the drop-down list.	The Web Scheduled Callback server must be in the Web domain. Select `Web` from the drop-down list if the server is in the Web domain.
Host	Select the machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

WSCallback tab

This tab does not have any advanced properties.

Field	Recommended entry	Notes
ICM Server Name	Enter the name of the machine where the ICM server is installed.	The WSC contacts are sent to the ICM server that you specify here.
Call Timeout Interval (sec)	Enter the number of seconds after which the request times out if it is not routed to an agent. Default is 120.	
IC Login	Enter the IC Login username. Default is dcobridge1	
IC Password	Select the Ellipsis (…) and specify the password for the IC Login.	

Field	Recommended entry	Notes
Advanced Properties		
Schedule Interval (sec)	Enter the number of seconds after which database polling for scheduling callback will begin. Default is 120.	
Call queue size	Enter the maximum number of callbacks that you can schedule at runtime. Default is 50. Minimum is 10 and Maximum is 200.	If you increase the Call queue size beyond 200, the WSC Server will restrict the queue size to maximum value of 200.
IC Data Source	Select the database source to use for database operations. Default is interaction_center.	
Data Network Pool Size	Read only field. Displays 100	Indicates the number of objects to be cached by the DCO Bridge.
Wait Time For Cache Ready	2000 (in msecs)	WSCallback will wait for the configured time (in milliseconds) before retrying for the cache to be ready.
Main Class	Read only field. Displays com/avaya/callback/WSCallback	Indicates the main class used by the WSCallback server.
Sysuser mode	Read only field. Displays 2	Indicates the Vesp User Mode used when logging to the Multi Threaded Toolkit (MTT).
Vespfactory classname	Read only field. Displays com.avaya.ie.vesp.VespFactory	Indicates the Vesp Bridge internal class used to implement the VespFactory interface.
Vesp interface	Read only field. Displays WSCallback	Indicates the Vesp interface used by the WSCallback server
Vesp localorb	Read only field. Displays false	Determines if the WSCallback server should copy the vesp.imp file from the primary machine and managed its updates.
Vesp requesthandler	Read only field. Displays com/avaya/callback/WSCallback	Indicates the default Vesp Request Handler used by the WSCallback server.

Field	Recommended entry	Notes
Send OrbReady	Read only field. Displays true	Sends a Ready signal to the ORB server.
Java ClassPath	Read only field. Display the java classpath.	

Debug tab

The Debug tab includes the following Web Scheduled Callback server specific parameters.

Field	Recommended entry	Notes
Log File	Enter the name of the file where the logfile is written for this server. Default is `wscallback.log`	
Log Level	Select the logging level. Default is 3.	

WebServices server

This section contains the following:

- General tab on page 554
- WebServices tab on page 554
- Debug tab on page 556

General tab

Field	Recommended entry	Notes
Name	WebServices_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya 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, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

WebServices tab

Field	Recommended entry	Notes
IC User	Enter the name of the agent account for this WebServices server.	Use the agent account that you created when you configured an agent account for WebServices.
IC Password	Enter the password of the agent account.	Use the password of the agent account that you created when you configured an agent account for WebServices.

Field	Recommended entry	Notes
Enable SSL for DS Authentication		If you select the **Enable SSL for DS Authentication** check box, the WebServices server send the DS.Authenticate request to DS over SSL in the SSL encrypted format. The SSL authentication is supported for both LDAP and non-LDAP users. If you clear the **Enable SSL for DS Authentication** check box, the WebServices server send the DS.Authenticate request to DS over VESP. In the case when you do not select this check box, the password will be in MD5 encrypted format and rest of the request parameter will be in plain text format. The VESP authentication is supported only for the non-LDAP users. Note: If you do not select the **Enable SSL for DS Authentication** check box, the DS.Authenticate request for the LDAP enabled users fails. To authenticate the LDAP enabled users, you must send the DS.Authenticate request over SSL by selecting the **Enable SSL for DS Authentication** check box.

Field	Recommended entry	Notes
Skip ADU Events for WebServices User	By default, the check box is not selected.	Select the check box if you want to skip receiving ADU events. You must restart the WebServices server after you select or clear the check box.

Debug tab

The Debug tab does not include any WebServices server specific parameters.

Workflow server

The Workflow server processes workflows that route contacts and implement business rules. The Workflow server can handle specific tasks, such as media routing, agent blending, agent scripts, letter generation, and generic business logic.

The Workflow server is enhanced to provide channel assignments through scripts. The Workflow server loads the Channel associations through the Synchronous Startup Flow or Startup Flows in the `<project_name>.<script_name>` format.

Below methods are the methods at a script level:

1. ChannelAssign String Range, String InterfaceName, String AssignCreteria

   For example, ChannelAssign "1", "TS", "*r50001"

2. ChannelAssociate String Range, String EventName, String FlowName

   For example, ChannelAssociate "1", "TS.IncomingCall", "ts.incomingcall"

These script extensions are used in a custom flow, which you can configure as a Synchronous Startup Flow or a Startup Flow. The channel assignment and event flow association information goes into these workflows.

You can configure the number of channel assignments for a workflow server using the couple name assigncount on the **Configuration** tab of the Workflow server. The maximum recommended value for the assigncount variable is 2047.

Note:
Configuring Channel assignments and event-flow associations through script is an additional option.

While configuring the Channel association and event flow association through scripts, the programmer must validate the uniqueness of Channel assign number range. The range of Channel association should match with ChannelAssign. If unique Ranges are not provided in the flow script the Workflow server does not start and logs the conditions.

You can execute the Workflows by directly invoking the Workflow or Workflows are executed as a result of receiving events from another server.

You can distribute these responsibilities across multiple Workflow servers to maximize performance and response from the server. For example, if your Avaya IC system includes multiple server systems, you can install secondary Workflow servers dedicated to specific media contacts on the secondary machines.

This section contains the following:

- General tab on page 557
- WorkFlow tab on page 558
- Channels tab on page 560
- Debug tab on page 563

General tab

Field	Recommended entry	Notes
Name	Workflow_<*domain*>	Include the domain in the server name to identify the server.
Domain	Select the Avaya 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 machine's IP address from the drop-down list, or enter the IP address if it is not in the list.	When you select the host, Avaya IC Manager fills in the fields for Directory, Port, and Executable.

WorkFlow tab

Field	Recommended entry	Notes
Reload Flows	Click 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 currently loaded flows even if the version numbers are the same.
Unload Flow	Click 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 increment the workflow version number. If the version has not been incremented, the workflow is not reloaded.
Run Flow	Click 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	Click 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.

Field	Recommended entry	Notes
Synchronous Startup Flows	Click 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	Click 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	Click the **Ellipsis (…)** and specify the list of semaphores used by the workflows.	For details about semaphores, see *Avaya IC Media Workflow Reference*.
Directory tables	Click the **Ellipsis (…)** and specify the Directory server tables to be loaded in the memory at startup.	
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: ● Instructed by Avaya Technical Support ● Debugging a workflow	This field is for debugging workflows only. Impacts performance of the Workflow server if checked. 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.

Field	Recommended entry	Notes
Advanced Properties		
Enable DB Access	Select this check box if you want to load the workflow from the database, or if your workflows require database access during processing.	If this check box is cleared, the server loads the workflows from the directory specified in the Flow Directory field and does not establish a connection with the database. If your workflows do not need to access the database, clearing this option can make them run more efficiently. If you select this check box, you should also select Database from the Script Source drop-down list.
Script Source	Select one of the following from the drop-down list: ● Database ● File	Default is Database. Specifies whether the workflow server should obtain workflows from the database or from a file.
Flow Directory	Accept the default of "flows" unless you have stored the workflows in another directory.	The name of the directory from which flows are loaded.
Worker Threads	Accept the default of 64 or enter a new value greater than 64.	The number of threads that should be dedicated to workflow execution.
Event Threads	Accept the default 10 or enter new value.	
Backup Length	Accept the default of 10 or enter a new value from 0 to 255.	Specifies how many previous blocks are remembered for use with the "go back" capability of Script.SetNextConnection. Range is 0 to 255. 0 disables the ability to go back, which can yield improved security and efficiency.
Enable Java Support For Script	Select this check box to enter the information for java class.	

Channels tab

The Channels tab lets you specify which flow should be run when a particular event is received by the Workflow server. You can access the Channel Editor and Channel Association dialog boxes from the Channels tab. The following examples show the recommended entries for the voice channel.

Channel Editor dialog box fields

Field	Recommended entry	Notes
Global	• Do not select this check box to create a channel for a specific server or media, such as voice or email. • Select this check box to create a channel that is not related to a specific media or server. **Note:** When you select this field, the other fields on the **Channel Editor** dialog box are greyed out and unavailable.	Use the **Global** field to create a global channel and association. Global channels allow you to specify associations between events and workflows that need to be handled uniformly, no matter where the request originates. The Workflow server tries any event or special request that is not media-specific against global channels. If you need the Workflow server to handle an event that is not media-specific, create a global channel and an association between the event and workflow in the global channel. For example, check the **Global** field to create a channel to handle IVR workflow requests from the VOX server, as described in *VOX Server Programmer Guide*.
By Server	• Do not select this check box 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 check box if you want this channel to handle events from only one the specific server that you select from the **Service** drop-down list.	If you check this field, and you need this Workflow server to communicate with more than one server, you must create another channel for that server. **Warning:** Do not check this field if you want the Workflow server to handle events from a server that has the same name as the server type. For example, if you check this field and select a Telephony server named “TS”, the Workflow server will not be able to communicate with that Telephony server.
Channel Range	No entry necessary.	Completed by Avaya IC Manager

Field	Recommended entry	Notes
Service	Select a server or type of server 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	Enter 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 *IC Telephony Connectors Programmer Guide*.

Channel Association dialog box fields

Field	Recommended entry	Notes
Channel Range		Completed by Avaya IC Manager
Service Interface		Completed by Avaya IC Manager
Event	Enter the name of the event that triggers the workflow in the **Flow** field.	For example, for the voice channel, enter: TS.IncomingCall **Note:** This field is case-sensitive.
Flow	Enter the contact routing workflow for the channel as *<workflow_project>.<routing_workflow>*	For example, if you use the sample workflow, enter `ts.incomingcall` **Note:** This field is case-sensitive.

Debug tab

You can access the following Workflow server specific debug parameters on the Debug tab:

Field	Recommended entry	Notes
Data Query Log Level	Select a number from 0 to 4, where 0 is the lowest level of logging and 4 is the highest.	Default is 0. Because logging requires system resources, you should select a minimal logging level unless you are trying to diagnose a specific problem.
Variables In Status	Select this check box if you need to debug the server.	A flag that determines if the current values of global server variables (Script.GlobalSet) are copied to the results of a GetStatus method.
Synchronous Execution	Select this check box only if advised by support personnel.	If sporadic failures are experienced, checking this option is a first step in isolating the problem. This forces the server to avoid allowing multiple threads to execute simultaneously by sharing the VM during idle periods. **Note:** Checking this option can adversely affect performance.
Assign Count	Accept the default or enter a number for the count.	Specifies how many Assignments you plan to use with the Association mechanism. The default is 2047, which is almost always adequate, and can be decreased to save a little memory. Raising this value lets the server handle more associations, which may be useful for large, multiprocessor systems handling multiple phone switches.

Field	Recommended entry	Notes
Enable Print	Check this option if you need to debug the server.	When checked, print statements are written to the log file. The default for this parameter is unchecked because writing print statements to the log file is costly in terms of system execution time. This parameter can be enabled to debug the server using print statements.
Trace Execution of Flows	Select this check box only if you need to debug the workflows run by this server.	When checked, this parameter traces the execution of flows on the system to tell you how long each block takes to run and how much time the thread spends blocked while waiting for something to become available.

Recommended server parameter settings

See the *IC Tunablle Parameters* topic in the *Performance specifications* chapter in *Avaya Interaction Center and Avaya Operational Analyst Overview and Specification* guide if your call center has the following contact volume:

- 15,000 voice calls per hour
- 1,000 emails per hour
- 1000 chats per hour

You can use these settings as a baseline to help you tune your own Avaya IC system.

Note:
For information about setting Configuration tab parameters, see Configuration tab on page 70.

Configuration Tool settings

To set the appropriate web configuration settings:

1. From the Windows **Start** menu, select **Programs** > **Avaya Interaction Center 7.3.x** > **Config Tool**.
2. On the **Web** tab, right-click and select **Show Advanced Properties**.
3. Set the following parameters (which appear at the bottom of the Config Tool dialog box) as shown:
   - **Website JVM options:** `--JvmMS256m --JvmMx1024m`

- **ICM JVM options:** `-Xms128m -Xmx512m`

4. Click **Apply Settings**.

For details about the Configuration Tool, see *IC Installation and Configuration*.

Appendix D: Typing special characters

If you want to add one of the following special characters to a topic keyword or in a sample email, press and hold the ALT key and enter the associated four digit code on your numeric keypad:

Character	Description	Character Code
€	Euro Sign	0128
¡	Inverted exclamation	0161
¢	Cent sign	0162
£	Pound sterling	0163
¤	General currency sign	0164
¥	Yen sign	0165
¦	Broken vertical bar	0166
§	Section sign	0167
¨	Umlaut (diaeresis)	0168
©	Copyright	0169
ª	Feminine ordinal	0170
«	Left angle quote, guillemotleft	0171
¬	Not sign	0172
	Soft hyphen	0173
®	Registered trademark	0174
¯	Macron accent	0175
°	Degree sign	0176
±	Plus or minus	0177
²	Superscript two	0178
³	Superscript three	0179
´	Acute accent	0180
µ	Micro sign	0181

Character	Description	Character Code
¶	Paragraph sign	0182
·	Middle dot	0183
¸	Cedilla	0184
¹	Superscript one	0185
º	Masculine ordinal	0186
»	Right angle quote, guillemotright	0187
¼	Fraction one-fourth	0188
½	Fraction one-half	0189
¾	Fraction three-fourths	0190
¿	Inverted question mark	0191
À	Capital A, grave accent	0192
Á	Capital A, acute accent	0193
Â	Capital A, circumflex accent	0194
Ã	Capital A, tilde	0195
Ä	Capital A, dieresis or umlaut mark	0196
Å	Capital A, ring	0197
Æ	Capital AE dipthong (ligature)	0198
Ç	Capital C, cedilla	0199
È	Capital E, grave accent	0200
É	Capital E, acute accent	0201
Ê	Capital E, circumflex accent	0202
Ë	Capital E, dieresis or umlaut mark	0203
Ì	Capital I, grave accent	0204
Í	Capital I, acute accent	0205
Î	Capital I, circumflex accent	0206
Ï	Capital I, dieresis or umlaut mark	0207
Ð	Capital Eth, Icelandic	0208

Character	Description	Character Code
Ñ	Capital N, tilde	0209
Ò	Capital O, grave accent	0210
Ó	Capital O, acute accent	0211
Ô	Capital O, circumflex accent	0212
Õ	Capital O, tilde	0213
Ö	Capital O, dieresis or umlaut mark	0214
×	Multiply sign	0215
Ø	Capital O, slash	0216
Ù	Capital U, grave accent	0217
Ú	Capital U, acute accent	0218
Û	Capital U, circumflex accent	0219
Ü	Capital U, dieresis or umlaut mark	0220
Ý	Capital Y, acute accent	0221
Þ	Capital THORN, Icelandic	0222
ß	Small sharp s, German (sz ligature)	0223
à	Small a, grave accent	0224
á	Small a, acute accent	0225
â	Small a, circumflex accent	0226
ã	Small a, tilde	0227
ä	Small a, dieresis or umlaut mark	0228
å	Small a, ring	0229
æ	Small ae dipthong (ligature)	0230
ç	Small c, cedilla	0231
è	Small e, grave accent	0232
é	Small e, acute accent	0233
ê	Small e, circumflex accent	0234
ë	Small e, dieresis or umlaut mark	0235

Character	Description	Character Code
ì	Small i, grave accent	0236
í	Small i, acute accent	0237
î	Small i, circumflex accent	0238
ï	Small i, dieresis or umlaut mark	0239
ð	Small eth, Icelandic	0240
ñ	Small n, tilde	0241
ò	Small o, grave accent	0242
ó	Small o, acute accent	0243
ô	Small o, circumflex accent	0244
õ	Small o, tilde	0245
ö	Small o, dieresis or umlaut mark	0246
÷	Division sign	0247
ø	Small o, slash	0248
ù	Small u, grave accent	0249
ú	Small u, acute accent	0250
û	Small u, circumflex accent	0251
ü	Small u, dieresis or umlaut mark	0252
ý	Small y, acute accent	0253
þ	Small thorn, Icelandic	0254
ÿ	Small y, dieresis or umlaut mark	0255

Appendix E: Property descriptions

This section describes the default properties that are built into Avaya IC. Some of the properties already have values, but others need to be customized for your contact center. Contact center properties should be assigned to the Avaya IC top-level entity, designated as **IC**. For more information about working with properties, see Chapter 15: Properties on page 364.

The out-of-the-box properties are assigned to property sections that correspond to the functional unit that uses them in Avaya IC Manager. Property sections help you organize the properties in Avaya IC Manager.

This section includes the following topics:

- Admin property descriptions on page 570
- Agent property descriptions on page 574
- Contact/AgentDesktop property descriptions on page 631
- Email property descriptions on page 632
- QUI property descriptions on page 633
- System/Configuration property descriptions on page 644
- Voice/Configuration property descriptions on page 646

Admin property descriptions

This section describes the administrative properties and includes the following topics:

- Admin/Agent properties on page 570
- Admin/Agent/Channel properties on page 572
- Admin/General properties on page 573
- Admin/Server properties on page 573

Admin/Agent properties

The following section describes the agent-related administrative properties.

EnableDisplayNameField

Description: Enables the Display Name field in the Agent Editor.

This field can be used in a localized environment when Avaya IC Manager cannot reliably build the agent's full name from the standard name fields.

By default, if this field is not visible or it is empty, an IC Script combines the agent's First and Last Name fields and enters that information into the database in the Display Name field. For details on changing the IC Script, see *IC Database Designer Application Reference*.

Default value: No

Use with: Avaya IC Manager

EnableMonitor

Description: Enables Avaya IC Manager to monitor agent state changes.

Default value: Yes

Use with: Avaya IC Manager

EnablePrefixSuffixVisible

Description: Enables the extended name fields prefix, suffix, and salutation in the Agent Editor.

Along with EnableDisplayNameField, this property is used for localized environments if Avaya IC Manager cannot build this information from other fields in the system. If you enable this property, you may need to change the default IC Script.

Default value: No

Use with: Avaya IC Manager

ForeignTextEntry

Description: Lets agents enter foreign text into certain server, agent, and DS Table configuration fields.

Default value: *No default set*

Use with: Avaya IC Manager

TaskCeilingDefault

Description: Default agent level task ceiling for a newly created agent. This value is used to restrict the agent's task load value.

Default value: 1

Use with: Avaya IC Manager

TaskLoadDefault

Description: Default agent level task load for a newly created agent. This value is used to restrict the total number of contacts that an agent can receive.

Default value: 1

Use with: Avaya IC Manager

Admin/Agent/Channel properties

The Chat, Email, and Voice channels all contain similar configuration properties. The following section describes the Admin/Agent/*Channel* properties.

ChannelEnabled

Description: Defines if a newly created agent should have access to this media channel. A value of Yes enables the channel for the agent, and a value of No disables the channel for the agent.

Default value: No

Use with: Avaya IC Manager

TaskCeilingDefault

Description: Determines the default task ceiling for a newly created agent

Default value: 1

Use with: Avaya IC Manager

TaskLoadDefault

Description: Determines the default task load for a newly created agent

Default value: 1

Use with: Avaya IC Manager

Admin/General properties

The following section describes the Avaya IC Manager properties.

ChatChannelEnabled

Description: Enable/Disable chat channel support.

Default value: Yes

Use with: Avaya IC Manager

EmailChannelEnabled

Description: Enable/Disable email channel support.

Default value: Yes

Use with: Avaya IC Manager

VoiceChannelEnabled

Description: Enable/Disable voice channel support.

Default value: Yes

Use with: Avaya IC Manager

Admin/Server properties

The following section describes the server administration properties.

EnableDebuggingDefault

Description: This property enables/disables debug level logging for any server instantiated.

Default value: No

Use with: Avaya IC Manager

EnableVoiceServerNotification

Description: This property enables/disables voice server notification.

Default value: Yes

Use with: Avaya IC Manager

Agent property descriptions

The following section describes the agent-related properties.

Note:
If you change any agent-related properties, the agent will need to log out and log back in before the changes will take effect.

This section includes the following topics:

- Agent properties on page 575
- Agent/Desktop properties on page 577
- Agent/Desktop/AddressBook properties on page 586
- Agent/Desktop/Chat properties on page 587
- Agent/Desktop/Chat/Application properties on page 588
- Agent/Desktop/ContactSuspension properties on page 590
- Agent/Desktop/CustomerContacts properties on page 591
- Agent/Desktop/Directory properties on page 592
- Agent/Desktop/Directory/SkillProficiency properties on page 595
- Agent/Desktop/Directory/Voice properties on page 596
- Agent/Desktop/Email properties on page 597
- Agent/Desktop/Email/AlertInfo/REQ properties on page 599
- Agent/Desktop/Email/AlertInfo/SME properties on page 600
- Agent/Desktop/Email/Application properties on page 601
- Agent/Desktop/Prompter properties on page 605
- Agent/Desktop/QuickFind properties on page 606
- Agent/Desktop/Resources properties on page 606
- Agent/Desktop/ScreenPop properties on page 607
- Agent/Security properties on page 609
- Agent/Desktop/Softphone properties on page 611
- Agent/Desktop/Spelling properties on page 612

- Agent/Desktop/StatusBar properties on page 615
- Agent/Desktop/Voice properties on page 617
- Agent/Desktop/WAC properties on page 622
- Agent/Desktop/WebClient properties on page 624
- Agent/Desktop/WebClient/Connection properties on page 627
- Agent/Desktop/WebClient/Preferences properties on page 628
- Agent/Desktop/WrapUp properties on page 629
- Agent/Desktop/WrapUpDialog properties on page 630

Agent properties

The following section describes the agent properties.

FullnameOrder

Description: This property is used by Avaya IC Manager when new agents are created, and the client when showing agent names. This property controls the order in which the agent's first name and last name appear in the Fullname field. Choices are:

- <Firstname> <Lastname>
- <Lastname>, <Firstname>
- <Lastname> <Firstname>

Default value: <Lastname>, <Firstname>

Use with: Avaya Agent desktop, Avaya Agent Web Client

UICountryOrRegion

Description: The two-letter suffix representing a country or region. This property is used with the UILanguage property to determine the full locale of the agent user interface. The supported values are:

- DE
- US
- CO
- FR
- IT
- JP

- KR
- BR
- RU
- TH
- CN
- TW

Default value: US

Use with: Avaya Agent Web Client, and IC Client SDK

Related properties: UILanguage on page 576

UILanguage

Description: The two-letter suffix representing the language the agent uses for their user interface. This property is used with the UICountryOrRegion property to determine the full locale of the agent user interface. When loading layouts for the Avaya Agent Desktop Application, the UILanguage is appended to the Layout property to form the fully-qualified layout name. The supported suffixes are:

- de (German)
- en (English)
- es (Spanish)
- fr (French)
- it (Italian)
- ja (Japanese)
- ko (Korean)
- pt (Portuguese)
- ru (Russian)
- th (Thai)
- zh (Simplified Chinese)
- zt (Traditional Chinese)

Note:
If your contact center uses both Avaya Agent desktop, and Avaya Agent Web Client. Select zt for Traditional Chinese.

Default value: en

Use with: Avaya Agent desktop, Avaya Agent Web Client, and IC Client SDK

Related properties: UICountryOrRegion on page 575, and Layout on page 582

Agent/Desktop properties

The following section describes the properties that affect the behavior and appearance of the agent interface.

AgentStatisticsLoggingEnabled

Description: The agent statistics produced when enabling this property are for client research information only. It is statistics based on what the client thinks it has handled. For real reporting information use OA. If set to Yes, Avaya IC records agent statistics in the log file **ICAgentClient_<username>_AgentStatistics.log**.

Default value: Yes

Use with: Avaya Agent desktop

AllowBlendingModeChange

Description: This property is used in conjunction with the BlendingMode property to determine the type of blending the agent will use. You may use these two properties to control how you would like an agent to manage their workloads.

If AllowBlendingModeChange is set to *No*, the agent will not be able to move between Automatic and Manual Blending modes.

If AllowBlendingModeChange is set to *Yes*, the agent will be able to freely move between Automatic and Manual Blending modes.

Default value: No

Use with: Avaya Agent Web Client

Related properties: BlendingMode on page 580

AllowVoiceTrailing

Description: Voice Trailing is the ability for an agent to work on a contact of non-voice type while working on voice work at the same time. For example, if an Agent is talking to a customer, and works on a chat or email, that voice work is considered trailing. This property works in conjunction with PromptOnVoiceTrailingDisallowed.

If an agent is not allowed to work on two pieces of work at the same time, set this property to *No*.

If an Agent can work on voice work with contacts of other media types, set this property to *Yes*.

Default value: Yes

Use with: Avaya Agent Web Client, and IC Client SDK

Related properties: PromptWhenVoiceTrailingDisallowed on page 584

AuxGroup

Description: If this property is enabled, this property is the name of the AuxGroup that will be used for returning the Agents Auxiliary and Logout Reason codes. This property is used with AuxGroupTenant for locating the set of codes to load from the IC system. For more information about configuring codes, see Creating wrap up, AuxWork, and Logout codes on page 308.

Default value: *No default set*

Use with: Avaya Agent desktop, Avaya Agent Web Client, and IC Client SDK

Related properties: AuxGroupTenant on page 578, AuxReasonCodesEnabled on page 579, and LogoutReasonCodesEnabled on page 583

AuxGroupTenant

Description: The Tenant for the Auxiliary Group to be used for the Agent's Reason or Logout Codes. See AuxGroup for more information.

Default value: *No default set*

Use with: Avaya Agent desktop, Avaya Agent Web Client, and IC Client SDK

Related properties: AuxGroup on page 578, and AuxReasonCodesEnabled on page 579

AuxLoginReasonCode

Description: The default Reason Code when an agent goes into AuxWork immediately upon logging in. This code is part of the AuxGroup specified in the SystemAuxGroup property.

If you change this value, you will need to change the values of the system codes so each code has a unique value. For more information, see Changing the default system AuxWork codes on page 315.

Default value: 0

Use with: Avaya Agent desktop, Avaya Agent Web Client, and IC Client SDK

Related properties: AuxWorkOnLogin on page 580, SystemAuxGroup on page 584, and SystemAuxGroupTenant on page 585

AuxLogoutReasonCode

Description: The default Reason Code when an agent goes into AuxWork immediately upon logging out. This code is part of the AuxGroup specified in the SystemAuxGroup property.

If you change this value, you will need to change the system codes to a unique value. For more information, see Changing the default system AuxWork codes on page 315.

Default value: 1

Use with: Avaya Agent desktop, Avaya Agent Web Client, and IC Client SDK

Related properties: SystemAuxGroup on page 584, and SystemAuxGroupTenant on page 585

AuxNotAvailableReasonCode

Description: The default Reason Code when an agent goes into AuxWork but has not selected an AuxWork reason for him or herself. This code is part of the AuxGroup specified in the SystemAuxGroup property.

If you change this value, you will need to change the values of the system codes so each code has a unique value. For more information, see Changing the default system AuxWork codes on page 315.

Default value: 1

Use with: Avaya Agent desktop, Avaya Agent Web Client, and IC Client SDK

Related properties: SystemAuxGroup on page 584, and SystemAuxGroupTenant on page 585

AuxReasonCodesEnabled

Description: Turns on Reason Code entry when entering AuxWork. Even if you do not enable AuxReasonCodes, System Aux Reason codes are used for writing the default codes for situations where you enter AuxWork.

Default value: No

Use with: Avaya Agent desktop, Avaya Agent Web Client, and IC Client SDK

Related properties: AuxGroup on page 578, and AuxGroupTenant on page 578

AuxReasonRequired

Description: Says that a Reason is required when going into AuxWork.

Note:
This property is not used for Avaya Agent Web Client, but the UI behavior is affected. If AuxReasonCodesEnabled are set to Yes for Avaya Agent Web Client, then an Aux Reason will always be required.

Default value: No

Use with: Avaya Agent desktop

Related properties: AuxGroup on page 578, AuxGroupTenant on page 578, and AuxReasonCodesEnabled on page 579

AuxRonaReasonCode

Description: The default Reason Code that is recorded when an agent goes into AuxWork through RONA. This code is part of the AuxGroup specified in the `SystemAuxGroup` property.

If you change this value, you need to change the values of the system codes, so that each code has a unique value. For more information, see Changing the default system AuxWork codes on page 315.

Note:
The **AuxRonaReasonCode** works only if IC is integrated with Business Advocate application for voice channel.

Default value: 1

Use with: Avaya Agent desktop, Avaya Agent Web Client, and IC Client SDK

Related properties: SystemAuxGroup on page 584

AuxWorkOnLogin

Description: Puts the agent in AuxWork when they login so that they will not receive any contacts. If set to No, then the agent will be made available immediately upon login.

Important:
This property should be used with caution. If set to *No*, an Agent will potentially receive contacts as soon as the channel has been logged into.

Default value: Yes

Use with: Avaya Agent desktop, and Avaya Agent Web Client

Related properties: AuxLogoutReasonCode on page 579

BlendingMode

Description: If `Automatic`, the maximum number of allowable tasks per channel is set by the system, and any change an agent makes to their availability affects all channels.

If `Manual`, the maximum number of tasks per channel can be changed by the agent, and he or she can change availability on a per channel basis.

See AllowBlendingModeChange for more information.

Default value: Automatic

Use with: Avaya Agent desktop and Avaya Agent Web Client

Related properties: AllowBlendingModeChange on page 577

ChannelThrottleTime

Description: : ChannelThrottleTime is the delay introduced between one channel becoming available before the next channel in a sequence. Although the process continues to be asynchronous, setting sufficient Throttle time would ensure voice channel becomes available first.

Default value: 0

Use with: Avaya Agent Web Client, Siebel Native Client, and SDK Client

CheckAuxWorkOnLogout

Description: This makes sure the Agent has gone into AuxWork before logging out. When an agent requests to logout of Avaya Agent, and the agent is not in AuxWork, this property will cause the Agent to see a warning dialog describing the potential problems with exiting without being in AuxWork.

Default value: Yes

Use with: Avaya Agent desktop

ConfirmBeforeRelease

Description: When set to *Yes*, the agent receives a confirmation prompt after selecting the **Release** toolbar button and before releasing the contact.

Default value: No

Use with: Avaya Agent Web Client

ContactSuspensionEnabled

Description: An agent may be prompted to suspend active contacts when this property is set to yes, and depending on the individual settings in the Agent/Desktop/ContactSuspension section.

When a contact arrives, Avaya Agent will analyze all the work currently in the agent's desktop. If there is work arriving and work on another channel that is active, then the agent’s system will display a prompt. The agent will be prompted to decide if they would like to suspend the other work so they can work immediately on the alerting item. This property does not allow the agent to automatically answer the incoming work. This property only allows the agent to suspend the other work. The Agent/Desktop/ ContactSuspension properties allow you to turn this behavior on or off for certain channels.

Default value: Yes

Use with: Avaya Agent desktop

Related properties: Agent/Desktop/ContactSuspension properties on page 590

DefaultContactHistoryRecordCount

Description: The default number of records that will be returned when the agent does a Contact History browser search. The agent can override this default using the Contact History Filter.

Default value: 10

Use with: Avaya Agent desktop

Related properties: MaxRecordCount on page 592

DisplayTime

Description: Sets whether date/times will be shown in Local or UTC time.

Default value: Local

Use with: Avaya Agent Web Client

IntegratedApplication

Description: This determines which 3rd-party application is integrated with Avaya Agent. See *Avaya Agent Integration* for more information about this property.

Default value: None

Use with: Avaya Agent desktop

Layout

Description: This property specifies which layout (CDL file) to use for Avaya Agent. When Avaya IC searches for this file, it takes the name you specify here and appends the two-letter language suffix specified in the UILanguage property. See *Avaya Agent Integration* for more information about this property.

Default value: avaya_agent

Use with: Avaya Agent desktop

Related properties: UILanguage on page 576

LogoutNotAvailableReasonCode

Description: Sets the reason code that is automatically entered for the Log Out reason when the system logs the agent out before the agent selects a reason

Note:
This code name must match the name of a logout code exactly.

Default value: 1

Use with: Avaya Agent Web Client, and IC Client SDK

Related properties: SystemAuxGroup on page 584, SystemAuxGroupTenant on page 585, and LogoutReasonCodesEnabled on page 583

LogoutReasonCodesEnabled

Description: Turns on Logout Code entry when logging out of Avaya Agent. Even if you do not enable AuxReasonCodes, System Aux Reason codes are used for writing the default codes for situations where you enter AuxWork.

Default value: No

Use with: Avaya Agent desktop, Avaya Agent Web Client, and IC Client SDK

Related properties: AuxGroup on page 578, and AuxGroupTenant on page 578

LogoutReasonRequired

Description: Says that a Reason is required when logging out of Avaya Agent.

Default value: No

Use with: Avaya Agent desktop, and Avaya Agent Web Client

Related properties: AuxGroup on page 578, AuxGroupTenant on page 578, and LogoutReasonCodesEnabled on page 583

MaxLoginRetryCount

Description: When logging into Avaya Agent, this is the number of times to allow the Agent to retry.

Default value: 3

Use with: Avaya Agent desktop

MultimediaEnabled

Description: When set to *Yes*, the agent can receive and initiate multimedia contacts.

Default value: Yes

Use with: Avaya Agent desktop, and Avaya Agent Web Client

PromptWhenVoiceTrailingDisallowed

Description: When set to *Yes* and AllowVoiceTrailing is set to *No*, an agent receives a prompt before the application places the voice contact on hold. See AllowVoiceTrailing for more information.

Default value: No

Use with: Avaya Agent Web Client

Related properties: AllowVoiceTrailing on page 577

ReportServerName

Description: Most of the time it is sufficient to have this property set to use the default value. The default setting ensures that the agent's regular failover definition is used when the Avaya Agent needs to communicate with the Report server. If there is a business need for an agent's requests to go to a specific Report server, then enter the name of a specific Report server.

Default value: Report

Use with: Avaya Agent desktop

ScreenPopEnabled

Description: Turns Screen Pops on and off for an Agent. Screen Pops almost always require some type of customization. See *Avaya Agent Integration* or *Avaya Agent Web Client Customization* for more information.

Default value: No

Use with: Avaya Agent desktop, and Avaya Agent Web Client

Related properties: Agent/Desktop/ScreenPop properties on page 607

SystemAuxGroup

Description: The AuxGroup that contains the AuxLoginReasonCode and the AuxNotAvailableReasonCode.

Default value: SystemAuxGroup

Use with: Avaya Agent desktop, Avaya Agent Web Client, and IC Client SDK

Related properties: SystemAuxGroupTenant on page 585

SystemAuxGroupTenant

Description: The tenant containing the SystemAuxGroup.

Default value: DefaultTenant

Use with: Avaya Agent desktop, Avaya Agent Web Client, and IC Client SDK

Related properties: SystemAuxGroup on page 584

VirtualQueueTransferFlowName

Description: Name of the flow that is used by the system when an Agent initiates a collaboration with a Virtual Queue. The Virtual Queue Transfer Flow is a very specialized flow. Any changes should be done to the out of the box flow with caution.

Default value: sys_transfer.transfertovq

Use with: Avaya Agent Web Client, and IC Client SDK

WrapUpEnabled

Description: Turns WrapUp on and off. If turned on, then you need to set WrapUpType. For more information on how to configure different behaviors in wrap-up, see the Agent/Desktop/WrapUp properties.

Default value: No

Use with: Avaya Agent desktop, and Avaya Agent Web Client

Related properties: WrapUpType on page 585, Agent/Desktop/Prompter properties on page 605, Agent/Desktop/WrapUp properties on page 629, and Agent/Desktop/WrapUpDialog properties on page 630

WrapUpType

Description: There are several different types of wrap-up supported in Avaya Agent:

- None - Wrap-up is enabled, but no code collection mechanism will be used. *None* is only supported in the Web Client

- Other - This is for collecting wrap-up codes through customization. See *Avaya Agent Integration* or *Avaya Agent Web Client Customization* for more information.
- Prompter - Prompter will be used for collecting wrap-up codes. See Agent/Desktop/Prompter section for related settings. *Prompter* is not supported in Web Client
- Siebel - Siebel will be used for collecting wrap-up codes. See *Avaya IC for Siebel 8 Integration* for more information.
- WrapUpDialog - Wrap-up dialog will be used for collecting wrap-up codes. See the Agent/Desktop/WrapUpDialog properties for more information.

Default value: WrapUpDialog

Use with: Avaya Agent desktop, and Avaya Agent Web Client

Related properties: WrapUpType on page 585, Agent/Desktop/Prompter properties on page 605, Agent/Desktop/WrapUp properties on page 629, and Agent/Desktop/WrapUpDialog properties on page 630

Agent/Desktop/AddressBook properties

This section describes the properties for defining the behavior of the **Address Book** in the agent interface.

AutoFilteringEnabled

Description: When set to *Yes*, the **Address Book** filters addresses based on the channel.

Default value: Yes

Use with: Avaya Agent Web Client

Related properties: Use the Agent/Desktop/Directory property, DisableFiltering on page 592 for the Avaya Agent desktop application.

FilteredViewSet

Description: This is the name of the FilteredViewSet to use for the Address Book.

Default value: DefaultViewSet

Use with: Avaya Agent Web Client, and IC Client SDK

MaxRecordCount

Description: This sets the maximum number of records to retrieve from the Database for each view.

Default value: 100

Use with: Avaya Agent Web Client, and IC Client SDK

Agent/Desktop/Chat properties

The following section describes the properties for defining the behavior of chat in the agent interface.

AllowDecline

Description: When set to *Yes*, an agent can decline chat work when it arrives.

Default value: No

Use with: Avaya Agent Web Client

AutoAccept

Description: When set to *Yes*, work is automatically accepted upon arrival. The following rules apply when this property is set to *Yes*:

- A contact will automatically be accepted and made current if there is no other current contact
- A voice contact will be delivered alerting if there is already another contact current
- An email or chat contact will be accepted but will be made inactive if there is already another contact current when the work is received.

When set to *No*, the following rules apply for manually accepting work:

- Manually accepting a contact will make it current if there is no other current contact
- Manually accepting a voice contact when there is already another current contact will make the newly accepted contact current, while making the other contact inactive
- Manually accepting an email or chat contact when there is already another current contact will not make it current. The contact will be inserted into the work list as inactive. The previously current contact will remain current in this case.

Default value: No

Use with: Avaya Web Client, and IC Client SDK

CollaborationTimeout

Description: The time in seconds to timeout a collaboration request that did not reach the WACD or if no response or acknowledgement was received from the WACD. Collaboration will not timeout if another agent is not available to take the request as long as the WACD received and queued the request successfully. After this occurs, the only way out is to cancel the collaboration request.

Default value: 60

Use with: Avaya Agent Web Client, and IC Client SDK

PromptOnArrival

Description: When set to *Yes*, an agent receives a confirmation prompt every time work arrives. This is meant to be similar to reminder dialogs. Each dialog that appears will be displayed cascaded from the top left corner of the Agent's desktop. These dialogs remains until either:

- The Agent clicks Yes or No
- The work item related to the dialog is removed from the Avaya Agent Web Client work list

Default value: No

Use with: Avaya Agent Web Client

RONATimeout

Description: The time in seconds to wait before redirecting work. If you would like to turn RONA off for this channel, you may set this to *0*. However, it is important to remember that if RONA is configured on the WACD server side, a work item may still RONA even if this property is set to *0*. The Agent Timeout in the WACD should be greater than the RONATimeout.

Default value: 0

Use with: Avaya Agent Web Client, and IC Client SDK

Related properties: AutoAccept on page 587

Agent/Desktop/Chat/Application properties

The following section describes the application-specific properties of chat in the agent interface.

AgentWaitingThreshold

Description: If the Agent sent the last message in a chat, then after this number of seconds, the text in the Agent waiting column of the Chat work list will turn red.

Default value: 30

Use with: Avaya Agent Web Client

CustomerWaitingThreshold

Description: If the customer sent the last message in a chat, then after this number of seconds, the text in the Customer Waiting column of the Chat work list will turn red.

Default value: 10

Use with: Avaya Agent desktop, and Avaya Agent Web Client

SendMessageOnEnter

Description: When set to *Yes*, will send the message immediately when an agent presses **Enter**. When set to *No*, the agent must press **Send** to send the message.

Default value: Yes

Use with: Avaya Agent Web Client

SendResourceOnDoubleClick

Description: When set to *Yes*, the agent's system immediately sends a resource when an agent double clicks an item.

When set to *No*, the agent can preview the resource in its respective text field and must insert the resource into the chat session and select the **Send** button.

Default value: No

Use with: Avaya Agent Web Client

ShowOnCurrent

Description: When set to *Yes*, the agent's system displays the Chat application window when making a chat current.

Default value: Yes

Use with: Avaya Agent Web Client

ShowOnLogin

Description: When set to *Yes*, the agent's system displays the Chat application at Login.

Default value: No

Use with: Avaya Agent Web Client

ShowOnSelect

Description: When set to *Yes*, the agent's system displays the Chat Application window when the agent selects a chat contact in the **Work List**.

Default value: No

Use with: Avaya Agent Web Client

SpellCheckOnSend

Description: When set to *Yes*, the agent's system automatically spell checks the message an agent types before the message is sent to a customer.

Default value: Yes

Use with: Avaya Agent Web Client

ShowTypingStatus

Description: When set to *Yes*, the chat client window displays the chat typing status of an agent to a customer and chat typing status of a customer to an agent.

Default value: No

Use with: Avaya Agent Web Client

TypingStatusThreshold

Description: The system displays the chat typing status for the time that you configured in this property.

Default value: 12 seconds

Use with: Avaya Agent Web Client

Agent/Desktop/ContactSuspension properties

The following section describes the properties that define how contact suspension works in Avaya Agent desktop.

PromptForArrivingChat

Description: When a contact arrives on the chat channel, Avaya Agent will check for contacts on other channels. See ContactSuspensionEnabled for more information.

Default value: Yes

Use with: Avaya Agent desktop

Related properties: ContactSuspensionEnabled on page 581

PromptForArrivingEmail

Description: When a contact arrives on the email channel, Avaya Agent will check for contacts on other channels. See ContactSuspensionEnabled for more information.

Default value: Yes

Use with: Avaya Agent desktop

Related properties: ContactSuspensionEnabled on page 581

PromptForArrivingVoice

Description: When a contact arrives on the voice channel, Avaya Agent will check for contacts on other channels. See ContactSuspensionEnabled for more information.

Default value: Yes

Use with: Avaya Agent desktop

Related properties: ContactSuspensionEnabled on page 581

Agent/Desktop/CustomerContacts properties

The following section describes the properties for defining the behavior of customer contacts in Avaya Agent Web Client.

DefaultListFilter

Description: Possible values for this are:

- Last 5 Contacts - Shows the last 5 contacts only
- Last 10 Contacts - Shows the last 10 contacts only
- Today - Shows contacts received today

- Yesterday - Shows contacts received yesterday (12:00 AM to 11:59:59 PM)
- Last 7 Days - Shows contacts received in the last 7 days
- This Week - Shows contacts received this week
- Last Week - Shows contacts received last week (12:00 AM first day of last week to 11:59:59 PM the last day of last week)
- This Month - Shows contacts received this month
- All Dates - Show all contacts received

Important:
Use the All Dates setting with caution

Default value: Last 5 Contacts

Use with: Avaya Agent Web Client

MaxRecordCount

Description: Sets the maximum number of customer contacts to retrieve from the database

Tip:
This property is used to prevent slow system performance on unconstrained searches.

Default value: 100

Use with: Avaya Agent Web Client, and IC Client SDK

Related properties: Use the Agent/Desktop property, DefaultContactHistoryRecordCount on page 582 for the Avaya Agent desktop application.

Agent/Desktop/Directory properties

The following section describes the properties that determine the behavior of the Directory server, the Unified Agent Directory (UAD) in Avaya Agent desktop or the Address Book in Avaya Agent Web Client.

Note:
The name UAD was changed to Address Book for the Avaya Agent Web Client interface.

DisableFiltering

Description: If set to Yes, then filtering will be disabled when agents search on the UAD.

Default value: No

Use with: Avaya Agent desktop

Related properties: Use the Agent/Desktop/AddressBook property, AutoFilteringEnabled on page 586 for the Avaya Agent Web Client application.

FetchSearchFlowName

Description: The name of the workflow that should be used to fetch the records found in response to a search on the UAD.

Default value: sys_agentsearch.fetch

Use with: Avaya Agent desktop

ShowAgentsOnStartup

Description: Shows the Agents tab in the UAD. If set to *No,* the Agents tab is not visible in the UAD.

Default value: No

Use with: Avaya Agent desktop

ShowAgentState

Description: If set to Yes, then the Agents state will be shown in the Directory tree.

Default value: Yes

Use with: Avaya Agent desktop

ShowAllAgents

Description: Shows entire Agent Directory Tree.

Default value: No

Use with: Avaya Agent desktop

SkillsSupport

Description: Used to enable the use of Skills in the Directory Find functionality.

Default value: Yes

Use with: Avaya Agent desktop

StartSearchFlowName

Description: The name of the workflow that starts a search on the UAD.

Default value: sys_agentsearch.start

Use with: Avaya Agent desktop

StopSearchFlowName

Description: The name of the workflow that stops the search on the UAD.

Default value: sys_agentsearch.stop

Use with: Avaya Agent desktop

TransferFlowName

Description: The name of the workflow that retrieves a destination from a virtual queue.

Default value: sys_transfer.transfertovq

Use with: Avaya Agent desktop

Related properties: Use the Agent/Desktop property, VirtualQueueTransferFlowName on page 585 for the Avaya Agent Web Client application.

UADStringFormat

Description: The format in which agent names will be displayed in the UAD's directory tree.

Default value: Standard

Use with: Avaya Agent desktop

WorkFlowServerName

Description: Name of the WorkFlow server that the Agent Directory uses to run flows.

Default value: *No default set*

Use with: Avaya Agent desktop

Agent/Desktop/Directory/SkillProficiency properties

The following section describes the properties that affect the use of skill proficiencies with Avaya Agent desktop.

ExpertMax

Description: Maximum value for Expert Skill Proficiency.

Default value: 10

Use with: Avaya Agent desktop

Related properties: SkillsSupport on page 593

ExpertMin

Description: Minimum value for Expert Skill Proficiency.

Default value: 10

Use with: Avaya Agent desktop

Related properties: SkillsSupport on page 593

HighMax

Description: Maximum value for High Skill Proficiency.

Default value: 9

Use with: Avaya Agent desktop

Related properties: SkillsSupport on page 593

HighMin

Description: Minimum value for High Skill Proficiency.

Default value: 7

Use with: Avaya Agent desktop

Related properties: SkillsSupport on page 593

LowMax

Description: Maximum value for Low Skill Proficiency.

Default value: 3

Use with: Avaya Agent desktop

Related properties: SkillsSupport on page 593

LowMin

Description: Minimum value for Low Skill Proficiency.

Default value: 1

Use with: Avaya Agent desktop

Related properties: SkillsSupport on page 593

MediumMax

Description: Maximum value for Medium Skill Proficiency.

Default value: 6

Use with: Avaya Agent desktop

Related properties: SkillsSupport on page 593

MediumMin

Description: Minimum value for Medium Skill Proficiency.

Default value: 4

Use with: Avaya Agent desktop

Related properties: SkillsSupport on page 593

Agent/Desktop/Directory/Voice properties

The following section describes the voice-specific properties related to the UAD in Avaya Agent desktop.

BlindTransferEnabled

Description: Enables/Disables the ability to do Blind Transfers.

Default value: Yes

Use with: Avaya Agent desktop

ConferenceEnabled

Description: Enables/Disables the ability to do Conferences.

Default value: Yes

Use with: Avaya Agent desktop

ConsTransferEnabled

Description: Enables/Disables the ability to do Consultative Transfers.

Default value: Yes

Use with: Avaya Agent desktop

Agent/Desktop/Email properties

The following section describes the properties that affect the behavior of Email in the agent's interface.

AllowDecline

Description: When set to *Yes*, the agent can decline work when it arrives. This property does not apply if AutoAccept is set to *Yes*.

Default value: No

Use with: Avaya Agent Web Client, and IC Client SDK

Related properties: AutoAccept on page 598

AllowLogoutWithEmail

Description: If set to Yes, agents can logout even if they have emails waiting in their email queue.

Default value: Yes

Use with: Avaya Agent desktop, and Avaya Agent Web Client

AutoAccept

Description: When set to *Yes*, work is automatically accepted upon arrival. Consider the following when this property is set to *Yes*:

- A contact will automatically be accepted and made current if there is no other current contact
- A voice contact will be delivered alerting if there is already another contact current
- An email or chat contact will be accepted but will be made inactive if there is already another contact current when the work is received.

When set to *No*, the following rules apply for manually accepting work:

- Manually accepting a contact will make it current if there is no other current contact
- Manually accepting a voice contact when there is already another current contact will make the newly accepted contact current, while making the other contact inactive
- Manually accepting an email or chat contact when there is already another current contact will not make it current. The contact will be inserted into the work list as inactive. The previously current contact will remain current in this case.

Default value: Yes

Use with: Avaya Agent Web Client, and IC Client SDK

Related properties: PromptOnArrival on page 598

FilterPoolsByTenant

Description: When set to *Yes*, the view of agents is restricted to only the pools of the tenant associated with the agent's primary workgroup. This is a new property introduced in Avaya IC 7.3.6. Prior to 7.3.6, there was no functionality to restrict selection of outbound email pool for an agent.

If the FilterPoolsByTenant property is left as *No*, which is the default value, agents can see all the pools.

In case of any changes to this property or pools in IC Manager, it is necessary to re-login to AARC.

Default value: No

Use with: Avaya Agent Rich Client

PromptOnArrival

Description: When set to *Yes*, the agent receives a confirmation prompt every time work arrives. This is meant to be similar to reminder dialogs. Each dialog that appears will be displayed cascaded from the top left corner of the Agent's desktop. These dialogs will remain until either:

- The Agent clicks Yes or No

- The work item related to the dialog is removed from the Avaya Agent Web Client work list

If AutoAccept and PromptOnArrival are both are set to *Yes*, then the user is prompted on arrival of a new email work item only if there is not already a current contact.

Default value: No

Use with: Avaya Agent Web Client

Related properties: AutoAccept on page 598

RONATimeout

Description: The time in seconds to wait before redirecting work. If you would like to turn RONA off for this channel, you may set this to *0*. However, it is important to remember that if RONA is configured on the server side, a work item may still RONA even if this is set to *0*.

Note:
IC does not provide any build in protection against excessively large email messages. Excessively large email message may degrade system performance. To insure proper operation, Avaya recommends that you configure your POP3 server so that it doesn't route excessively large email messages into the IC system, but instead sends it to a separate email box for review. Excessively large email messages may also affect client response time during work delivery and handling. Therefore, Avaya also recommends that you configure the Agent/Desktop/Email/RONATimeout agent property appropriately based on your email handling needs.

Default value: 30

Use with: Avaya Agent Web Client, and IC Client SDK

Agent/Desktop/Email/AlertInfo/REQ properties

The following section describes the properties that affect agent emails requesting more information from customers.

AlertDuration

Description: Time to wait for Alert to fire in seconds.

Default value: 86400

Use with: Avaya Agent desktop, and Avaya Agent Web Client

SendToAnyAgent

Description: If set to Yes, responses to the email may go to any agent.

Default value: Yes

Use with: Avaya Agent desktop, and Avaya Agent Web Client

SetAlert

Description: If set to Yes, an Alert will be set for the Email.

Default value: No

Use with: Avaya Agent desktop, and Avaya Agent Web Client

Agent/Desktop/Email/AlertInfo/SME properties

The following section describes the properties that affect emails sent from an agent to a Subject Matter Expert (SME).

AlertDuration

Description: Time to wait for Alert to fire.

Default value: 86400

Use with: Avaya Agent desktop, and Avaya Agent Web Client

SendToAnyAgent

Description: If set to Yes, responses to the email may go to any agent.

Default value: Yes

Use with: Avaya Agent desktop, and Avaya Agent Web Client

SetAlert

Description: If set to Yes, and Alert will be set for the Email.

Default value: No

Use with: Avaya Agent desktop, and Avaya Agent Web Client

Agent/Desktop/Email/Application properties

The following section describes the application-specific properties of email in Avaya Agent Web Client.

AutoSaveEnabled

Description: When set to *Yes*, the Email application automatically saves email composition drafts.

Default value: Yes

Use with: Avaya Agent Web Client

Related properties: AutoSaveTime on page 601

AutoSaveTime

Description: When AutoSaveEnabled is set to *Yes*, the application automatically saves a copy of the email composition drafts at the specified minute interval.

Default value: 10

Use with: Avaya Agent Web Client

Related properties: AutoSaveEnabled on page 601

ConfirmBeforeSend

Description: When set to *Yes*, the agent receives a prompt from the system to confirm that they want to send the email after selecting the **Send** button.

Default value: No

Use with: Avaya Agent Web Client

OutboundCharsetDefault

Description: Specifies the default character set to use when an agent responds and the source character set cannot be used.

If UseOutboundCharsetDefault is set to *Yes*, then OutboundCharsetDefault specifies the character set used when an agent sends a response email and the original emails character set cannot be used. This setting also applies when the agent sends a new outbound email, because there is no original email to check.

If UseOutboundCharsetDefault is set to *No*, then the agent is prompted to select a character set in the above scenarios, with the default selection being the one specified in OutboundCharsetDefault.

Default value: *i*so-8859-15

Use with: Avaya Agent Web Client

Related properties: UseOutboundCharsetDefault on page 605

OutboundEmailAccountDefault

Description: Specifies the default email account to be used in Avaya Agent Web Client when an agent sends a new outbound email. Avaya Agent Web Client automatically populates the **From** field in all outbound emails with this email account.

If you want to specify a default email account for Avaya Agent Web Client, set the value of this property to the same email account that is defined in the **Email Accounts** dialog box of IC Manager.

Default value: *None.*

Use with: Avaya Agent Web Client

QuoteOriginalInResponse

Description: When set to *Yes*, the original message will appear in the email response. When set to *No*, the agent has the option of manually inserting a copy of the original message in the email response.

Default value: Yes

Use with: Avaya Agent Web Client

QuotePrefix

Description: Specifies the prefix that will be used when QuoteOriginalInResponse is set to *Yes*.

Default value: >

Use with: Avaya Agent Web Client

ReadInHTML

Description: If set to *Yes*, multipart/alternative inbound messages will display the HTML portion initially in the client. Otherwise, it will display the non-HTML section.

Default value: Yes

Use with: Avaya Agent Desktop, Avaya Agent Web Client

ReleaseOnAlert

Description: When set to *Yes*, the system releases work automatically after the agent sends an email composition for an email alert contact.

Default value: No

Use with: Avaya Agent Web Client

ReleaseOnExternalAgent

Description: When set to *Yes*, IC releases work automatically after the agent forwards an external agent's email composition.

Default value: No

Use with: Avaya Agent Web Client

ReleaseOnNOR

Description: When set to *Yes*, IC releases work automatically after sending a normal reply (NOR).

Default value: No

Use with: Avaya Agent Web Client

ReleaseOnREQ

Description: When set to *Yes*, IC releases work automatically after sending a response requesting further information (REQ).

Default value: No

Use with: Avaya Agent Web Client

ReplyOnActivate

Description: IC automatically opens a reply composition tab for the work item when an email becomes active and there is no type of response in progress.

Default value: No

Use with: Avaya Agent Web Client

SendAsHTML

Description: When set to *Yes*, sets the default mode of new outbound emails to HTML.

Default value: No

Use with: Avaya Agent Desktop, Avaya Agent Web Client

ShowOnCurrent

Description: IC displays the email application window when making an email current.

Default value: Yes

Use with: Avaya Agent Web Client

ShowOnLogin

Description: IC displays the Email application when the agent logs into their system.

Default value: No

Use with: Avaya Agent Web Client

ShowOnSelect

Description: IC displays the email application window when an agent selects an email in the work list.

Default value: No

Use with: Avaya Agent Web Client

SpellCheckOnSend

Description: When set to *Yes*, IC spell checks the email before sending it.

Default value: Yes

Use with: Avaya Agent Web Client

Related properties: Agent/Desktop/Spelling properties on page 612

SpellCheckOriginal

Description: When set to *Yes* and the original email is quoted in the response, IC spell checks the original email.

Default value: No

Use with: Avaya Agent Web Client

Related properties: Agent/Desktop/Spelling properties on page 612

UseOutboundCharsetDefault

Description: Controls what happens if an agent sends a new outbound email, replies to an email, or forwards an email, and IC cannot use the character set from the original email. If UseOutboundCharsetDefault is set to *Yes*, then Avaya Agent Web Client sends the email in the character set specified in the related property OutboundCharsetDefault. If UseOutboundCharsetDefault is set to *No*, then Avaya Agent Web Client prompts the agent to choose a character set for the outbound email. The character set specified in OutboundCharsetDefault will be the default answer to this prompt.

Default value: Yes

Use with: Avaya Agent Web Client

Related properties: OutboundCharsetDefault on page 601

WordWrapEnabled

Description: When set to *Yes*, IC enables word-wrap in the Email application.

Default value: Yes

Use with: Avaya Agent Web Client

Agent/Desktop/Prompter properties

The following section describes the properties that affect the behavior of Prompter in Avaya Agent desktop.

WrapUpFlow

Description: Flow that is used for WrapUp.

Default value: sample_wrapup

Use with: Avaya Agent desktop

Related properties: WrapUpEnabled on page 585, WrapUpType on page 585, WrapUpFlowset on page 605, and WrapupRequired on page 606

WrapUpFlowset

Description: Flowset that contains the WrapUp Flow.

Default value: prompter

Use with: Avaya Agent desktop

Related properties: WrapUpEnabled on page 585, WrapUpType on page 585, WrapUpFlow on page 605, and WrapupRequired on page 606

WrapupRequired

Description: If set to Yes, then the Agent will go through WrapUp.

Default value: No

Use with: Avaya Agent desktop

Related properties: WrapUpEnabled on page 585, WrapUpType on page 585, WrapUpFlow on page 605, and WrapUpFlowset on page 605

Agent/Desktop/QuickFind properties

The following section describes the properties for defining the behavior of quick find in Avaya Agent Web Client.

NumberOfEntriesToShow

Description: Specifies the maximum number of entries that the system can display in the **Quick Find** drop-down list.

Default value: 10

Use with: Avaya Agent Web Client, and IC Client SDK

NumberOfEntriesToStore

Description: Specifies the maximum number of Quick Find entries that can be stored in the Database.

Default value: 20

Use with: Avaya Agent Web Client

Agent/Desktop/Resources properties

The following section describes the properties for defining the behavior of resources in Avaya Agent Web Client.

MyResourcesEnabled

Description: When set to *Yes*, an agent can create his or her own resources.

Default value: Yes

Use with: Avaya Agent Web Client and Avaya Agent desktop

TemplateDownload

Description: In IC 7.3.2, TemplateDownload determines the templates available to the agent based on workgroup to folder mapping in RLManager. The possible values are All, Restrictive, and Selective.

- **All**: Agent is able to view and use templates from all email template folders.
- **Restrictive**: Agent is able to view and use only the email templates from the folders mapped to agent's workgroup. The agent cannot switch to any other view.
- **Selective**: Agent is able to view and use only the email templates from the folders mapped to agent's workgroup. However, agent can switch the view to use templates from all the folders.

Default value: All

StatusDownload

Description: Determines the set of resolve statuses available to the agent. The possible values are All, Restrictive.

- **All**: Agent will be able to view and use resolve status from all the folders.
- **Restrictive**: Agent will be able to view and use only the resolve statuses from the folders mapped to the agent's workgroup.

Default value: All

Note:

The following error message is displayed in the ICManager on deleting a Workgroup, if the workgroup is mapped to a folder or folders in RLManager:

Delete Operation cannot be performed: The selection of workgroup ["<Workgroup Name>"] is mapped with Email Template folders in RLManager.

Agent/Desktop/ScreenPop properties

The following section describes the properties that affect how screen pops are handled by the agent interface.

ClearFocusOnContactCompletion

Description: If Screen Pops are enabled and this property is set to Yes, then any focus that was backfilled as a result of the Screen Pop is cleared once the contact is completed.

Default value: No

Use with: Avaya Agent desktop

Related properties: ScreenPopEnabled on page 584

PopOnAllArrivingContacts

Description: Screen Pop occurs for all contacts arriving in Avaya Agent.

Default value: No

Use with: Avaya Agent desktop, and Avaya Agent Web Client

Related properties: ScreenPopEnabled on page 584

PopOnContactActivation

Description: Screen Pop occurs when contact is activated in Avaya Agent.

Default value: No

Use with: Avaya Agent desktop, and Avaya Agent Web Client

Related properties: ScreenPopEnabled on page 584

PopOnFirstArrivingContact

Description: Screen Pop occurs when there are no other contacts in Avaya Agent. FirstArriving has a special meaning in relation to this property. It does not necessarily mean that the Agent has no other work on their desktop. What this means is that there is no other active* work on the Agent's desktop. This property allows a Screen Pop to happen as a contact arrives, but only if the Agent is not working on something else in Avaya Agent. Therefore, when a contact arrives, Avaya Agent will analyze the other work currently present in the desktop and Screen Pop only if there isn't any other active work

> **Note:**
> In the Desktop Application, active means there are no contacts in the active state. In the Web Client, this means there is no current work.

Default value: Yes

Use with: Avaya Agent desktop, and Avaya Agent Web Client

Related properties: ScreenPopEnabled on page 584

Agent/Security properties

The following section describes the properties that affect the passwords agents can use, and how often those passwords need to be changed. The Directory server needs to be restarted for the changes to take effect. All Agent/Security properties can be disabled by setting the properties to *0*.

CAUTION:
The values you enter for these fields are not verified. Therefore you could make it impossible to create passwords if, for example, you specify that agents must use at least 5 alphabetic characters and 5 numeric characters and then specify a maximum password length of 8. Make sure that the values you enter do not conflict with one another.

ForcePasswordChange

Description: If set to Yes, this forces agents to change their password when they log in after a password change has been made in Avaya IC Manager. The exception to this is if PasswordReuseCycles is set to 0. The setting of 0 means there are no restrictions on password reuse. For details, see Agent passwords on page 227.

Default value: Yes

Use with: Avaya Agent desktop, and Avaya Agent Web Client

MaxLoginAttemptsAllowed

Description: The maximum number of times the agent can attempt to log in with incorrect passwords before Avaya IC disables the agent's account.

To re-enable the agent's account, the system administrator needs to clear the Disable Login check box on the Security tab of the Agent Manager. For more information, see Agent passwords on page 227.

Default value: 5

Use with: Avaya Agent desktop, and Avaya Agent Web Client

MaxPasswordLength

Description: The maximum number of alphanumeric characters you can use in a password.

Default value: 40

Use with: Avaya Agent desktop, and Avaya Agent Web Client

MinPasswordAlphabets

Description: The minimum number of alphabetic characters that you can use in a password.

CAUTION:
Make sure that this value combined with the value for MinPasswordNumerics does not exceed the setting for MaxPasswordLength.

Default value: 1

Use with: Avaya Agent desktop, and Avaya Agent Web Client

MinPasswordLength

Description: The minimum number of alphanumeric characters you can use in a password.

The value for this property must be greater than, or equal to, 1 (one). You cannot use blank passwords in Avaya IC.

CAUTION:
Make sure that this value does not exceed the setting for MaxPasswordLength.

Default value: 6

Use with: Avaya Agent desktop, and Avaya Agent Web Client

MinPasswordNumerics

Description: The minimum number of numeric characters that you can use in a password.

Make sure that this value combined with the value for MinPasswordAlphabets does not exceed the setting for MaxPasswordLength.

Default value: 1

Use with: Avaya Agent desktop, and Avaya Agent Web Client

NumOfDays

Description: The NumOfDays and NumOfPasswordChanges properties work together. Agents cannot change their password more times than specified in the length of time specified in NumOfDays.

For example, with the default settings, agents can only change their password 3 times in a single day.

Default value: 1

Use with: Avaya Agent desktop, and Avaya Agent Web Client

Related properties: NumOfPasswordChanges on page 611

NumOfPasswordChanges

Description: The NumOfDays and NumOfPasswordChanges properties work together. Agents cannot change their password more times than specified in NumOfPasswordChanges.

Default value: 3

Use with: Avaya Agent desktop, and Avaya Agent Web Client

Related properties: NumOfDays on page 610

PasswordChange

Description: Determines whether agents can change their password at runtime.

If you set this property to Yes, Avaya Agent users will have a Change Password option on the main agent interface.

Default value: No

Use with: Avaya Agent desktop, and Avaya Agent Web Client

PasswordChangeDuration

Description: The number of days before a password expires. If you want to specify that the password never expires, set this property to 0 (zero).

Default value: 60

Use with: Avaya Agent desktop, and Avaya Agent Web Client

PasswordReuseCycles

Description: The number of unique passwords that must be used before an agent can reuse a previous password.

Default value: 5

Use with: Avaya Agent desktop, and Avaya Agent Web Client

Agent/Desktop/Softphone properties

The following section describes the properties that define how Softphone works with Avaya Agent.

PromptForLogin

Description: If set to Yes, then an agent will always be presented with the Login dialog box for Softphone.

Tip:
You should use this option if agents log into different machines in your facility instead of having a dedicated workstation.

Default value: No

Use with: Avaya Agent desktop

PromptNextLogin

Description: If set to Yes, then an agent will be presented with the Login dialog box for Softphone the next time he or she logs in.

Tip:
If PromptForLogin is set to No, this property lets you force agents to re-log in once to accommodate any Softphone login changes.

Default value: *No default set*

Use with: Avaya Agent desktop

SwapHeldEnabled

Description: If set to Yes, then the ability to swap callers during Consultative Transfers and Conferences is enabled. This property may not work for some switches.

Default value: Yes

Use with: Avaya Agent desktop

Agent/Desktop/Spelling properties

The following section lists the properties for defining the behavior of spelling in Avaya Agent Web Client.

CaseSensitive

Description: When set to *Yes*, spell checking verifies that uppercase and lowercase letters are used correctly.

Default value: Yes

Use with: Avaya Agent Web Client

IgnoreCapitalizedWords

Description: When set to *Yes*, spell checking ignores words that begin with a capitalized letter.

Default value: No

Use with: Avaya Agent Web Client

IgnoreInternetAndFileAddresses

Description: When set to *Yes*, spell checking ignores internet and file addresses.

Default value: Yes

Use with: Avaya Agent Web Client

IgnoreWordsInMixedCase

Description: When set to *Yes*, spell checking ignores words with upper and lower case letters, but not words with a leading uppercase letter followed by lowercase letters.

Default value: No

Use with: Avaya Agent Web Client

IgnoreWordsInUppercase

Description: When set to *Yes*, spell checking ignores words that are all in uppercase letters.

Default value: No

Use with: Avaya Agent Web Client

IgnoreWordsWithNumbers

Description: When set to *Yes*, spell checking ignores words that contain numbers.

Default value: No

Use with: Avaya Agent Web Client

PreferredCountry

Description: Specifies the preferred country to use for spell checking. This property is used in conjunction with PreferredLanguage for spell checking. The supported values are:

- BR
- CO
- DE
- FR
- GB
- IT
- US

Default value: US

Use with: Avaya Agent Web Client

PreferredLanguage

Description: Specifies the preferred language to use for spell checking. This property is used in conjunction with PreferredCountry for spell checking. The supported values are:

- de
- en
- es
- fr
- it
- pt

Default value: en

Use with: Avaya Agent Web Client

ReportDoubleWords

Description: When set to *Yes*, spell checking verifies that there are no repeated words.

Default value: Yes

Use with: Avaya Agent Web Client

SuggestReplacements

Description: When set to *Yes*, spell checking provides suggestions for misspelled words. If set to No, the agent can request replacements for a particular misspelled word by selecting the **Suggest** button in the spell check dialog

Default value: Yes

Use with: Avaya Agent Web Client

SuggestSplitWords

Description: When set to *Yes*, spell checking provides suggestions on when to split words.

Default value: Yes

Use with: Avaya Agent Web Client

Agent/Desktop/StatusBar properties

The following section describes the properties for defining the behavior of the **Status Bar** in Avaya Agent Web Client.

ErrorTimeout

Description: Specifies the time in seconds that error messages (Error) will display in the **Status Bar**.

Default value: 30

Use with: Avaya Agent Web Client

InfoTimeout

Description: Specifies the time in seconds that informational status messages (Info) will display in the **Status Bar**.

Default value: 3

Use with: Avaya Agent Web Client

LogFileSize

Description: Specifies the maximum size of the Status Bar log file in bytes.

Note:
When the file reaches the specified number of bytes, the system will create a backup file and create a new file to log to.

Default value: 100000

Use with: Avaya Agent Web Client

MinimumMessageLevel

Description: Specifies the lowest level of message that will display in the **Status Bar**. The supported values are:

- Info
- Warning
- Error

Default value: Warning

Use with: Avaya Agent Web Client

MinimumPopupMessageLevel

Description: Specifies the lowest level of message that will cause the Status Bar Details window to display. The supported values are:

- Info
- Warning
- Error

Default value: Error

Use with: Avaya Agent Web Client

NumberOfMessagesToShow

Description: Specifies the number of messages that will display in the Details window of the Status Bar.

Default value: 25

Use with: Avaya Agent Web Client

PopupMessagesEnabled

Description: When set to *Yes*, IC turns PopUp messages on. If Popup messages are on, then the MinimumPopupMessageLevel setting determines which level of messages are displayed by the system.

Default value: No

Use with: Avaya Agent Web Client

WarningTimeout

Description: Specifies the time in seconds that warning messages (Warning) will display in the **status bar**.

Default value: 10

Use with: Avaya Agent Web Client

Agent/Desktop/Voice properties

The following section describes the properties for defining the behavior of voice in Avaya Agent Web Client.

AutoAcceptACD

Description: When set to *Yes*, the system will automatically accept ACD calls upon arrival. The following rules apply when this property is set to *Yes*:

- A contact will automatically be accepted and made current if there is no other current contact
- A voice contact will be delivered alerting if there is already another contact current
- An email or chat contact will be accepted but will be made inactive if there is already another contact current when the work is received.

When set to *No*, the following rules apply for manually accepting work:

- Manually accepting a contact will make it current if there is no other current contact
- Manually accepting a voice contact when there is already another current contact will make the newly accepted contact current, while making the other contact inactive
- Manually accepting an email or chat contact when there is already another current contact will not make it current. The contact will be inserted into the work list as inactive. The previously current contact will remain current in this case.

Default value: No

Use with: Avaya Agent Web Client, and IC Client SDK

AutoAcceptDirect

Description: When set to *Yes*, the system will automatically accept direct calls upon arrival. The following rules apply when this property is set to *Yes*:

- A contact will automatically be accepted and made current if there is no other current contact
- A voice contact will be delivered alerting if there is already another contact current
- An email or chat contact will be accepted but will be made inactive if there is already another contact current when the work is received.

When set to *No*, the following rules apply for manually accepting work:

- Manually accepting a contact will make it current if there is no other current contact
- Manually accepting a voice contact when there is already another current contact will make the newly accepted contact current, while making the other contact inactive
- Manually accepting an email or chat contact when there is already another current contact will not make it current. The contact will be inserted into the work list as inactive. The previously current contact will remain current in this case.

Default value: No

Use with: Avaya Agent Web Client, and IC Client SDK

AutoIn

Description: When set to *Yes*, an AutoIn-type behavior is enabled for the Voice channel. When a call is disconnected, the agent is immediately available for the next call.

Default value: No

Use with: Avaya Agent Web Client, and IC Client SDK

ConferenceEnabled

Description: When set to *Yes*, the Conference feature is on.

Default value: Yes

Use with: Avaya Agent Web Client, and IC Client SDK

ConsultEnabled

Description: When set to *Yes*, the Consultative Transfer feature is on.

Default value: Yes

Use with: Avaya Agent Web Client, and IC Client SDK

KeypadEnabled

Description: When set to *Yes*, agents can use the keypad.

Default value: No

Use with: Avaya Agent Web Client, and IC Client SDK

KeypadShowAlphanumeric

Description: When set to *Yes*, the system displays alphanumeric buttons in the keypad.

Default value: Yes

Use with: Avaya Agent Web Client

Related properties: KeypadEnabled on page 619

NoEDUEventCreationTimeout

Description: Specifies the time in milliseconds the Voice Channel will wait for the EDU event to arrive before creating the work.

Default value: 500

Use with: Avaya Agent Web Client, and IC Client SDK

NoTSEventCreationTimeout

Description: Specifies the time in milliseconds the Voice Channel will wait for the TS event to arrive before creating the work.

Default value: 2000

Use with: Avaya Agent Web Client, and IC Client SDK

PromptAndPersistNextLogin

Description: When set to *Yes*, the system prompts the agent for voice login information the next time the agent logs in.

This setting allows for login changes in an environment where PromptForLogin is not enabled. Information is stored in the Voice Channel record for the agent.

Default value: No

Use with: Avaya Agent Web Client, and IC Client SDK

PromptForLogin

Description: When set to *Yes*, the system prompts the agent for voice login information. This setting allows for free-seating.

Default value: No

Use with: Avaya Agent Web Client

PromptOnArrival

Description: When set to *Yes*, the system prompts the agent each time work arrives. This is meant to be similar to reminder dialogs. Each dialog that appears will be displayed cascaded from the top left corner of the Agent's desktop. These dialogs will remain until either:

- The Agent clicks Yes or No
- The work item related to the dialog is removed from the Avaya Agent Web Client work list

Default value: No

Use with: Avaya Agent Web Client

RONATimeout

Description: Specifies the time in seconds before the system redirects work. If you would like to turn RONA off for this channel, you may set this to *0*. However, it is important to remember that if RONA is configured on the server side, a work item may still RONA even if this is set to *0*.

This currently is ONLY supported when used in conjunction with Advocate.

Default value: 0

Use with: Avaya Agent Web Client, and IC Client SDK

SwapHeldEnabled

Description: When set to *Yes*, calls can be placed on hold when switching between an agent or a customer during either a consultive transfer call or a conference call. This functionality is enabled with the Move Conversation feature.

Important:
If the switch does not support the Move Conversation feature, this property must be set to *No*.

Default value: Yes

Use with: Avaya Agent Web Client

SwitchTimedACWEnabled

Description: When set to *Yes*, the Voice Channel works with timed ACW on the Switch.

Default value: No

Use with: Avaya Agent Web Client, and IC Client SDK

TransferEnabled

Description: When set to *Yes*, the Transfer feature is on.

Default value: Yes

Use with: Avaya Agent Web Client, and IC Client SDK

TransferType

Description: Specifies the type of transfer to be done. The two types of Transfer supported are:

- Single-Step - A single-step transfer uses a single request to the connector. This is a true blind transfer.
- Two-Step - A two-step transfer uses two requests to initiate and complete the connector. This is a consultative transfer with an automatic complete and better error handling.

Default value: Two-Step

Use with: Avaya Agent Web Client, and IC Client SDK

AllowTransferOnHold

Description: An agent can transfer, conference, or consult a call, which is currently on hold.

- Yes: An agent can transfer, conference, or consult the customer call, which is currently on hold.
- No: An agent cannot transfer, conference, or consult the customer call, which is currently on hold.

Default Value: No

Use with: Avaya Agent, Avaya Agent Web Client, IC Client SDK

ReconnectOnTransferCancel

Description: An agent is not automatically connected to a customer call, which is on hold, when the agent disconnects the consultation call with another agent.

- **Yes**: When the agent disconnects or cancels the conference or consultation call, the agent is automatically connected to the customer call.
- **No**: When the agent disconnects or cancels the conference or consultation call, the customer call is put on hold.

Default value: Yes

Use with: Avaya Agent, Avaya Agent Web Client, IC Client SDK

Agent/Desktop/WAC properties

The following section describes the properties that affect the behavior of the Web Agent with Avaya Agent.

AllowBlindTransfer

Description: Specifies whether agents perform a consulative transfer or a blind transfer or both. The values that an administrator can set are:

- 1 - Agents can perform consultative transfer only.
- 2 - Agents can perform blind transfers to queues only.
- 3 - Agents can perform both blind transfers and consultative transfers.

Default value: 1

Use with: Avaya Agent desktop

AppMode

Description: Mode of the Web Agent Client application.

Default value: avaya

Use with: Avaya Agent desktop

HomeDir

Description: The agent's home directory.

Default value: ../WebAgent

Use with: Avaya Agent desktop

ShowOnChatActivate

Description: If Yes, then the Web Agent client will appear when an agent activates a Chat. For example, when the agent double-clicks on the chat in the Chat task list.

Default value: Yes

Use with: Avaya Agent desktop

ShowOnChatSelect

Description: If Yes, then the Web Agent client will appear when an agent selects a chat task. For example, when the agent clicks on the chat in the Chat task list.

Default value: No

Use with: Avaya Agent desktop

ShowOnEmailActivate

Description: If Yes, then the Web Agent client will appear when an agent activates an email. For example, when the agent double-clicks on the email in the Email task list.

Default value: Yes

Use with: Avaya Agent desktop

ShowOnEmailSelect

Description: If Yes, then the Web Agent client will appear when an agent selects an email. For example, when the agent clicks on the email in the Email task list.

Default value: Yes

Use with: Avaya Agent desktop

TraceLevel

Description: This is a Debug Level for the Web Agent Client.

Default value: 9

Use with: Avaya Agent desktop

Agent/Desktop/WebClient properties

The following section describes the properties for defining the behavior of Avaya Agent Web Client.

BaseFont

Description: Specifies which font is used for the Avaya Agent Web Client user interface. The supported values are:

- Arial, sans-serif
- Arial, serif
- Georgia, sans-serif
- Georgia, serif
- Helvetica, sans-serif
- Helvetica, serif
- Times New Roman, sans-serif
- Times New Roman, serif
- Verdana, sans-serif
- Verdana, serif

Default value: Arial, sans-serif

Use with: Avaya Agent Web Client

BaseFontSize

Description: Specifies the font size that should be used for the Web Client UI. Use this property in conjunction with BaseFonts to make fonts "fit" well into the UI.

Default value: 11

Use with: Avaya Agent Web Client

DebugEnabled

Description: When set to *Yes*, enables debugging capabilities in the Web Client

Default value: No

Use with: Avaya Agent Web Client

DesktopPreferences

Description: Stores all the preferences from the desktop. For example, things like widget and window sizes and positions. DO NOT attempt to edit this field.

Default value: NA

Use with: Avaya Agent Web Client

LogLevelClient

Description: Specifies the level of logging for Avaya Agent Web Client on the client-side. The logging levels are:

- 6-Fatal - Logs Fatal level errors only
- 5-Error - Logs Error and Fatal level errors
- 4-Warning - Logs Warning, Error, and Fatal level errors
- 3-Info - Logs Info, Warning, Error, and Fatal level errors
- 2-Debug - Logs Debug, Info, Warning, Error, and Fatal level errors
- 1-Trace - Logs Trace, Debug, Info, Warning, Error, and Fatal level errors

Important:
Enabling lower levels of logging could result in performance degradation. For example, the Chat application may run out of memory if the log level is set to anything except 6-Fatal or 5-Error.

Default value: 5-Error

Use with: Avaya Agent Web Client

LogLevelServer

Description: Specifies the level of logging for Avaya Agent Web Client on the server-side. Setting the log level at a given number will result in logging at that level and all levels higher. This property only acts as a filter to the **log4j** file configuration of Avaya Agent Web Client.

- 1-Trace - Logs Trace, Debug, Info, Warning, Error, and Fatal level errors
- 2-Debug - Logs Debug, Info, Warning, Error, and Fatal level errors
- 3-Info - Logs Info, Warning, Error, and Fatal level errors
- 4-Warning - Logs Warning, Error, and Fatal level errors
- 5-Error - Logs Error and Fatal level errors
- 6-Fatal - Logs Fatal level errors only

Important:
Enabling lower levels of logging could result in performance degradation.

Default value: 5-Error

Use with: Avaya Agent Web Client, and IC Client SDK

Skin

Description: The name of the skin to use for Avaya Agent Web Client

Default value: avayaplain

Use with: Avaya Agent Web Client

TCDelay

Description: The TCDelay property specifies the time for TransferCancel delay in milliseconds to overcome the race condition between events from the switch, and events processed by Avaya Agent Web Client, in order to avoid customer dropping out of the call.

Note:
TCDelay will default to zero if its value is not specified. The recommended value of TCDelay is 1500 milliseconds (that is, 1.5 seconds). If Avaya Agent Web Client disconnects the call during consult/conference even after providing appropriate delay, then increment the TCDelay value in a step of 200 milliseconds and re-login the agent, this may be repeated until the appropriate delay time is reached where Avaya Agent Web Client does not disconnect the call.

Default Value: 0 (zero)

Use with: Avaya Agent Web Client, Avaya Agent Rich Client, and IC Client SDK

Template

Description: The name of the template to use for Avaya Agent Web Client

Default value: avaya_agent

Use with: Avaya Agent Web Client

WorkingDirectory

Description: This is the working directory for Avaya Agent Web Client. Avaya recommends you set this to a directory that is accessible from the Web Application Server. The Web Application Server is used to run the server side of Avaya Agent Web Client.

Default value: *No default set*

Use with: Avaya Agent Web Client, and IC Client SDK

Agent/Desktop/WebClient/Connection properties

The following section describes the properties for defining the behavior of the Avaya Agent Web Client connection to the application servers.

HeartBeatTimer

Description: The ping interval in seconds, for testing the client/server connectivity.

> **Important:**
> This must be set to a number less than the idle time out of the ADU Server servicing the agent's ADU.

You need to set the **`messaging.session.heartbeat`** property in the `Web.xml` file. You can find the `Web.xml` file at the following location: `icclientsuite\web\WebContent\WEB-INF`.

If the **`messaging.session.heartbeat`** property is not present in the Web.xml file, you can add the code for the heartbeat property as mentioned below:

```
<env-entry>
<description>The ping interval for testing the client/server
  connectivity. Default is 60 seconds. (Defined in MessagingDefs)</
  description>
<env-entry-name>messaging.session.heartbeat</env-entry-name>
<env-entry-value>60</env-entry-value>
<env-entry-type>java.lang.String</env-entry-type>
</env-entry>
```

Default value: 60

Use with: Avaya Agent Web Client

TrackEvents

Description: When set to *Yes*, statistics about events will be logged. This property is used only for development and support issues.

Default value: No

Use with: Avaya Agent Web Client

Agent/Desktop/WebClient/Preferences properties

Agent/Desktop/WebClient/Preferences contains dynamically generated persistence settings for agents. The actual properties that are in Agent/Desktop/WebClient/Preferences will be varied. Instances of these properties will only be created at the Agent level as the settings for a given agent are saved. To reset an Agent's settings, you should remove all property instances in Agent/Desktop/WebClient/Preferences.

Agent/Desktop/WebClient/Preferences/PreferredWorkload properties

Agent/Desktop/WebClient/Preferences/Preferred Workload contains agent preferred workload levels by media channel.

Chat

Description: Stores the agent preferred chat workload level; set by the agent in the Preferences dialog of Avaya Agent Web Client. Changes in the Preferences dialog overwrite the current value of this property

Default value: None, populates when the agent changes values in the Preferences dialog.

Use with: Avaya Agent Web Client

Related properties: BlendingMode on page 580 and AllowBlendingModeChange on page 577. Both of these properties must be set to true for this property to be used.

Email

Description: Stores the agent preferred email workload level; set by the agent in the Preferences dialog of Avaya Agent Web Client. Changes in the Preferences dialog overwrite the current value of this property

Default value: None, populates when the agent changes values in the Preferences dialog.

Use with: Avaya Agent Web Client

Related properties: BlendingMode on page 580 and AllowBlendingModeChange on page 577. Both of these properties must be set to true for this property to be used.

Voice

Description: Stores the agent preferred voice workload level; set by the agent in the Preferences dialog of Avaya Agent Web Client. Changes in the Preferences dialog overwrite the current value of this property

Default value: None, populates when the agent changes values in the Preferences dialog.

Use with: Avaya Agent Web Client

Related properties: BlendingMode on page 580 and AllowBlendingModeChange on page 577. Both of these properties must be set to true for this property to be used.

Agent/Desktop/WrapUp properties

The following section describes the properties for defining the behavior of WrapUp in Avaya Agent Web Client.

CollectCodesWhen

Description: Specifies when codes are collected within the WrapUp session. If you want to collect the codes at the beginning, set the property for `Start`. If you want to collect the codes at the end, set the property for `End`. The supported values are:

- Start - Codes are collected at the beginning of the wrap-up session.
- End - Codes are collected at the end of the wrap-up session.

Default value: Start

Use with: Avaya Agent Web Client

Related properties: WrapUpEnabled on page 585, and WrapUpType on page 585

CompleteAfterCodes

Description: When set to *Yes*, the application completes work automatically after the system collects the WrapUp codes. When set to *No*, the agent must use the **Complete** button to indicate all after contact work is finished.

If CollectCodesWhen is set to *End*, then CompleteAfterCodes does not affect the application.

Default value: Yes

Use with: Avaya Agent Web Client

Related properties: WrapUpEnabled on page 585, WrapUpType on page 585, and CollectCodesWhen on page 629

EnterWhen

Description: Specifies when the system enters the WrapUp phase. If you want the system to enter the WrapUp phase all the time, set the property for `Always`. If you want the system to enter the WrapUp phase at the end of each contact, set the property for `Selective`. The supported values are:

- Always - Wrap-up will always be entered at the end of a contact
- Selective - Whether to enter wrap-up or not is left up to the agent to decide

Default value: Always

Use with: Avaya Agent Web Client

Related properties: WrapUpEnabled on page 585, WrapUpType on page 585, and SelectiveDefault on page 630

SelectiveDefault

Description: Determines the initial state of requesting WrapUp or not when EnterWhen is set to *Selective*. The supported values are:

- Not Requested - When a contact arrives at the agent's desktop, the default will be to not enter wrap-up.
- Requested - When a contact arrives at the agent's desktop, the default will be to enter wrap-up.

Default value: Requested

Use with: Avaya Agent Web Client

Related properties: WrapUpEnabled on page 585, WrapUpType on page 585, and EnterWhen on page 630

Agent/Desktop/WrapUpDialog properties

The following section describes the properties that affect the behavior of the Wrap Up Dialog in the agent interface.

DefaultCategoryGroup

Description: The Default Category Group to use for WrapUp Codes.

Default value: *No default set*

Use with: Avaya Agent desktop, Avaya Agent Web Client, and IC Client SDK

Related properties: WrapUpEnabled on page 585, WrapUpType on page 585, and DefaultTenant on page 631

DefaultTenant

Description: The Default Tenant from which to retrieve Category Group for WrapUp Codes.

Default value: *No default set*

Use with: Avaya Agent desktop, Avaya Agent Web Client, and IC Client SDK

Related properties: WrapUpEnabled on page 585, WrapUpType on page 585, and DefaultCategoryGroup on page 631

Required

Description: If set to Yes, then the Agent is required to select a WrapUp code.

Default value: No

Use with: Avaya Agent desktop, and Avaya Agent Web Client

Related properties: WrapUpEnabled on page 585, and WrapUpType on page 585

Contact/AgentDesktop property descriptions

The following section describes the property that affects emails escalated from a tenant's web site.

TenantLogoURL

Description: The location of the tenant logo that Avaya IC should send when an email is escalated from the web site.

Default value: *No default set*

Use with: Avaya Agent desktop

Email property descriptions

The Email property section provides configuration and runtime information that is used by Email Management.

This section includes the following topics:

- Email/Agent properties on page 632
- Email/Runtime properties on page 632

Email/Agent properties

The following section describes the property that affects agent emails.

ReviewQuota

Description: Whole number percentage of outbound emails sent to review prior to delivery.

The outbound email workflow uses this value to determine what percentage of an agent's outbound emails needs to be approved by an approver. For details, see *Avaya IC Media Workflow Reference*.

Default value: 0

Use with: Avaya Agent desktop and Avaya Agent Web Client

Email/Runtime properties

The following section describes the Email Management runtime properties.

CurrentSequenceDate

Description: Do not modify, for system use only.

Default value: N/A

Use with: Avaya Agent desktop and Avaya Agent Web Client

CurrentSequenceNumber

Description: Do not modify, for system use only.

Default value: N/A

Use with: Avaya Agent desktop and Avaya Agent Web Client

LastConfigDump

Description: Do not modify, for system use only.

Default value: N/A

Use with: Avaya Agent desktop and Avaya Agent Web Client

RunningServerId

Description: Do not modify, for system use only.

Default value: N/A

Use with: Avaya Agent desktop and Avaya Agent Web Client

RunningServerName

Description: Do not modify, for system use only.

Default value: N/A

Use with: Avaya Agent desktop and Avaya Agent Web Client

QUI property descriptions

The QUI property descriptions includes the following topic:

- QUI/General properties on page 633

QUI/General properties

The following section describes the environmental properties.

AlertGracePeriod

Description: Determines the length of time that makes up the grace period when dealing with alerts.

Default value: 5

Use with: Avaya Agent desktop

AlertWindow

Description: Determines the position of the alert form in the following format: left/top/height/width.

Default value: 0|0|2100|15045

Use with: Avaya Agent desktop

AudibleAlerts

Description: Determines if a beep is played when an alert is received by the agent.

Default value: TRUE

Use with: Avaya Agent desktop

DebugLevel

Description: Determines the DCO debug level. This can be set to 0, 1, 2, or 3.

For clients and application servers:

- Errors only - 0
- Errors + warnings (default) - 1
- Errors + warnings + info - 2
- Errors + warnings + info + debug - 3

For Data servers:

- None - 0
- Open/close connections - 1
- All commands (i.e. all SQL) - 2
- All commands and return values - 3

Default value: 3

Use with: Avaya Agent desktop

EscalationAgent

Description: When using multiple QAlert Agents, specifies which agent receives escalations.

Default value: 1

Use with: Avaya Agent desktop

FaxClient

Description: Determines if client side fax integration is available. The FaxDefault property must be set to Client.

Default value: FALSE

Use with: Avaya Agent desktop

FaxDefault

Description: Determines the default fax to use. This property can be set to Client or Server. FaxMAPI and FaxServer are relevant only if FaxDefault is set to Server.

Default value: Server

Use with: Avaya Agent desktop

FaxMAPI

Description: Determines if MAPI fax is enabled. The FaxDefault property must be set to Server.

Default value: FALSE

Use with: Avaya Agent desktop

FaxServer

Description: Determines if a fax server is available. The FaxDefault property must be set to Server.

Default value: FALSE

Use with: Avaya Agent desktop

FaxServerAgent

Description: Determines the fax server agent. This property is set programmatically, do not change.

Default value: 2

Use with: Avaya Agent desktop

FaxServerName

Description: Specifies the name of the fax server machine.

Default value: Faxsvr

Use with: Avaya Agent desktop

ForeignFieldItalics

Description: Determines how to display foreign fields labels and contents. True display them in italics. False displays foreign fields the same as other labels or controls.

Default value: TRUE

Use with: Avaya Agent desktop

HTMLForm

Description: Determines the position of the HTML form in the following format: left/top/height/width.

Default value: *No default set*

Use with: Avaya Agent desktop

InitialFoci

Description: Determines the first focus that is displayed when the application starts up.

Default value: *No default set*

Use with: Avaya Agent desktop

LTSplit

Description: Determines the top position of the splitter in a long text field.

Default value: 4500

Use with: Avaya Agent desktop

MailDefault

Description: Determines the default setting to use for mail. The values for this property are Client or Server. MailServer and MailServerAgent are relevant only if MailDefault is set to Server.

Default value: Server

Use with: Avaya Agent desktop

MailMAPI

Description: Determines whether MAPI mail is available. The MailDefault property must be set to Server. More information is available in the *Avaya Agent Integrator's Guide*.

Default value: FALSE

Use with: Avaya Agent desktop

MailServer

Description: Determines if server mail is available. The MailDefault property must be set to Server.

Default value: TRUE

Use with: Avaya Agent desktop

MailServerAgent

Description: Specifies the ID of the QAlert agent to use for server mail. Used for QAlert running on UNIX only.

Default value: 2

Use with: Avaya Agent desktop

MaxForms

Description: Determines the maximum number of the application's focuses that can be open at one time.

Default value: 10

Use with: Avaya Agent desktop

MaxRecords

Description: Determines the maximum number of records that can be retrieved when a search is performed.

Default value: 100

Use with: Avaya Agent desktop

OldStyleButtons

Description: Determines the shape of the button in the application. If set to True, the buttons are displayed in a rectangular shape.

Default value: FALSE

Use with: Avaya Agent desktop

PagerClient

Description: Determines if client side pager integration is available. The PagerDefault property must be set to Client.

Default value: FALSE

Use with: Avaya Agent desktop

PagerDefault

Description: Pagers can be used for escalation and normal notification events. For escalation events, the page is fired through Notification server. Custom IC Scripts must be written to handle these notifications. Escalations through Notification server are included out-of-the-box. This setting specifies the location of the pager software which sends pager notifications.

The property's values are Server and Client:

- Server indicates that Notification server triggers pager notifications.
- Client indicates that the client's pager software sends notifications.

Default value: Server

Use with: Avaya Agent desktop

PagerServer

Description: Determines whether to use QAlert to trigger pager notification. PagerDefault property must be set to Server.

Default value: FALSE

Use with: Avaya Agent desktop

PagerServerAgent

Description: If your environment has multiple Notification server instances, use this setting to specify the Notification server agent that triggers pager notifications.

Default value: 2

Use with: Avaya Agent desktop

PagerServerEmail

Description: Determines whether to use Notification server to trigger Pager Email notification. The PagerDefault property must be set to Serveremail.

Default value: FALSE

Use with: Avaya Agent desktop

PagerServerName

Description: Determines the name of the pager server machine.

Default value: Pagesvr

Use with: Avaya Agent desktop

PollForAlerts

Description: Determines whether the agent is configured to poll for alerts.

Default value: TRUE

Use with: Avaya Agent desktop

PollingInterval

Description: Determines the interval at which the agent polls for alerts. The agent must be configured to poll for alerts with the PollForAlerts property enabled.

Default value: 1

Use with: Avaya Agent desktop

PrintClient

Description: Determines whether a client-side print server integration is available. The PrintDefault property must be set to Client.

Default value: FALSE

Use with: Avaya Agent desktop

PrintDefault

Description: Sets the default printer. This property can be set to Client or Server. A client uses the printers that are defined on the client machine, and a server uses only the printers that are defined on the server machine.

Default value: Client

Use with: Avaya Agent desktop

PrintServer

Description: Determines if print server is available. The PrintDefault property must be set to Server.

Default value: FALSE

Use with: Avaya Agent desktop

PrintServerAgent

Description: Specifies the printer to be used as the default printer in an environment with multiple print servers.

Default value: 2

Use with: Avaya Agent desktop

PrintServerName

Description: Determines the name of the print server.

Default value: Printsvr

Use with: Avaya Agent desktop

QScriptWindow

Description: Sets the position of the IC Script form using the format: left|top|height|width.

Default value: *No default set*

Use with: Avaya Agent desktop

ReportServerAgent

Description: Specifies the QAlert agent that triggers scheduled reports in an environment that has multiple Notification server instances, use this setting to specify Notification server agent that triggers scheduled reports.

Default value: 3

Use with: Avaya Agent desktop

ReuseDeletedFocuses

Description: Determines the number of focuses to be saved for reuse.

Default value: 5

Use with: Avaya Agent desktop

ReuseDeleteFocusInstances

Description: Determines how many focus instances are saved for reuse.

Default value: 3

Use with: Avaya Agent desktop

SeverityList

Description: Specifies the list of enumerated strings for the Severity column on the application starting from low.

Default value: Low|Medium|High|Critical|Special

Use with: Avaya Agent desktop

ShowBatchAdministrator

Description: Determines access control for the Batch Administrator. False denies access.

Default value: TRUE

Use with: Avaya Agent desktop

ShowLinkIcon

Description: Determines whether to display link icons for 1:M relation.

Default value: FALSE

Use with: Avaya Agent desktop

ShowReportWriter

Description: Determines access control for the Report Writer. False denies access to the Report Writer.

Default value: TRUE

Use with: Avaya Agent desktop

ShowSQL

Description: Determines access control for the SQL menu option. False denies access to this option.

Default value: TRUE

Use with: Avaya Agent desktop

ShowWorkSchedule

Description: Determines access control for the Work Scheduler. False denies access to the Work Scheduler.

Default value: TRUE

Use with: Avaya Agent desktop

SQLTextWindow

Description: Determines the position of the SQL text form in the following format: left/top/height/width.

Default value: *No default set*

Use with: Avaya Agent desktop

Title

Description: This property is no longer used by Avaya IC.

Default value: *No default set*

Use with: Avaya Agent desktop

TypeLibraries

Description: Registers all of the specified Type Libraries.

Default value: *No default set*

Use with: Avaya Agent desktop

UseDefaultControlHeight

Description: Determines if the design time height setting is overridden.

Default value: TRUE

Use with: Avaya Agent desktop

UseForeignSearchNULL

Description: Determines if NULL is used in foreign search speciality.

Default value: TRUE

Use with: Avaya Agent desktop

WordWrap

Description: Determines if word wrap is enabled in long text fields.

Default value: FALSE

Use with: Avaya Agent desktop

WordWrapCol

Description: Determines the column position where word wrap occurs.

Default value: 70

Use with: Avaya Agent desktop

WorkSchedule

Description: Determines the work schedule for the site. This is set programmatically. Change with caution.

Default value: *No default set*

Use with: Avaya Agent desktop

System/Configuration property descriptions

The following section describes the system settings for Avaya IC.

ChatLoginServer

Description: Specifies the hostname of the chat web site server. For Avaya IC Manager and Web site integration to work, you must change the default value.

Default value: %WEBLINK_SERVER%.%WEBLINK_DOMAIN%

Use with: Avaya IC Manager

ChatLoginServerPort

Description: Specifies the port number used by the chat web site server. Typically uses 80 for non-secure HTTP and 443 for HTTPs.

Default value: 80

Use with: Avaya IC Manager

ChatLoginServerProtocol

Description: Specifies the protocol used by the chat web site server. Typically uses http or https.

Default value: http

Use with: Avaya IC Manager

ChatLoginServerWebsite

Description: Specifies the chat website. This is the virtual directory of the web site.

Default value: website

Use with: Avaya Agent desktop

EmailLoginServer

Description: Specifies the server that hosts the login page for the Email Template Administration website. For Avaya IC Manager and Web site integration to work, you must change the default value.

Default value: %IMC_SERVER%.%IMC_DOMAIN%

Use with: Avaya IC Manager

EmailLoginServerPort

Description: Specifies the port number used by the server that hosts the login page for the Email Template Administration website. Typically uses 80 for non-secure HTTP and 443 for HTTPS.

Default value: 80

Use with: Avaya IC Manager

EmailLoginServerProtocol

Description: Specifies the protocol used by the server that hosts the login page for the Email Template Administration website. Typically uses HTTP or HTTPS.

Default value: http

Use with: Avaya IC Manager

EmailLoginServerWebsite

Description: Specifies the virtual directory of the Email Template Administration website.

Default value: rlmanager

Use with: Avaya IC Manager

EmailServer

Description: Specifies the hostname of the Email Management server. For Avaya IC Manager and Web site integration to work, you must change the default value.

Default value: %IMC_SERVER%.%IMC_DOMAIN%

Use with: Avaya Agent desktop

EmailServerPort

Description: The port number used by the Email Management server for Mail Template Administration.

Default value: 19114

Use with: Avaya Agent desktop

EnableContentAnalysis

Description: Alerts the system that Content Analysis should be used when processing Email.

Default value: *No default set*

Use with: Avaya Agent desktop

Voice/Configuration property descriptions

The following section describes the MTT configuration properties.

autoloadimp

Description: Enables or disables the automatic loading of the implementation file when the client machine is started. The implementation file will be downloaded to the client machine every time an agent logs into the Avaya Agent application.

Default value: True

Use with: Avaya Agent desktop

autoloadint

Description: Enables or disables the automatic loading of the interface repository file when the client machine is started. The implementation file will be downloaded to the client machine every time an agent logs into the Avaya Agent application.

If need to add a custom server, you must either:

- Set this option to True for each client (or for a workgroup or the entire system) and then log in under each client's ID, or
- Manually copy `vespidl.pk` to each client's machine.

Once you have updated all of the client desktops with the custom server, Avaya recommends that you reset this property to False in order to improve startup performances.

Default value: True

Use with: Avaya Agent desktop

logfilesize

Description: The size in bytes the log file can grow to. Valid range is between 1K and 50MB.

Default value: 25000000

Use with: Avaya Agent desktop

ronatimeout

Description: Sets the Redirect On No Answer time for calls.

Default value: 0

Use with: Avaya Agent desktop

Related properties: Use the Agent/Desktop/Voice property, RONATimeout on page 620 for the Avaya Agent Web Client application.

ServerFailureRetryCount

Description: The number of times Avaya IC should try to Assign a contact to a VESP server if it receives a server failed event.

Default value: 100000

Use with: Avaya Agent desktop

ServerFailureWaitDuration

Description: The number of milliseconds to wait between VESP server retries.

Default value: 5000

Use with: Avaya Agent desktop

trace

Description: Enables various levels of MTT logging for agents. More than one value can be specified by entering values separated by a comma, for example idl,flush. The trace values are:

- idl - log vesp requests to and replies from IC servers
- flush - flush logs immediately to logs
- explain - fail-over logic explained for each request in the logs
- shiptime - tell when a request is actually shipped on the wire from agent client machine
- timing - log elapsed time for each vesp request

Default value: *No default set*

Use with: Avaya Agent desktop

Index

A

account.text.userprop tenant property 333
accounts
  Admin 235
  creating for customers 334
  dcobridge 235
  default management process 337
  disabling customer 337
  icmbridge 235
  modifying customer 335
  website 235
AcdName table 145, 146
actions, and the support role 230
Add Samples tab 178
AddCustomer workflow. 337
adding
  email filters 123, 124
  new configuration records 137
  properties to user accounts 333
  servers. 74
address, specifying for an agent 218
Admin account. 235
admin default account 29
admin properties. 570
admin/agent properties. 570
admin/agent/channel properties. 572
admin/general properties 573
admin/server properties 573
Administrator role 229
ADU server
  about 420
  configuration parameters 420
  defined. 64
Advocate
  activating for agents 233
agent
  contacts handled by. 203
agent activity, viewing 200
Agent Editor 216
Agent History tab 223
Agent Manager 214, 215
Agent Notes tab 223
agent properties 575
Agent role 230
agent/desktop properties 577
agent/desktop/AddressBook properties 586
Agent/Desktop/Chat 587
Agent/Desktop/Chat/Application 588
agent/desktop/contactsuspension properties 590
Agent/Desktop/CustomerContacts 591
agent/desktop/directory properties 592
agent/desktop/directory/skillproficiency properties . 595
agent/desktop/directory/voice properties 596
agent/desktop/email properties 597
agent/desktop/email/alertinfo/req properties 599
agent/desktop/email/alertinfo/sme properties 600
Agent/Desktop/Email/Application 601
agent/desktop/prompter properties. 605
Agent/Desktop/QuickFind properties 606
Agent/Desktop/Resources properties 606
agent/desktop/screenpop properties 607
agent/desktop/softphone properties 611
Agent/Desktop/Spelling properties 612
Agent/Desktop/StatusBar properties 615
Agent/Desktop/Voice properties 617
agent/desktop/wac properties 622
Agent/Desktop/WebClient properties. 624
Agent/Desktop/WebClient/Connection properties . . 627
Agent/Desktop/WebClient/Preferences properties . 628
Agent/Desktop/WebClient/Preferences/PreferredWorkload properties. 628
agent/desktop/wrapup properties 629
agent/desktop/wrapupdialog properties 630
agent/security properties 609
Agent_Search table. 150
AgentEmailDrafts.xml file 298
Agentname macro 104
AgentPreferences.xml file 298
AgentResources.xml file 297
agents
  activating Advocate 233
  adding custom information 234
  adding notes for 223
  and failover order 222
  and queues 376
  assigning passwords 227
  assigning properties to. 230
  assigning roles and privileges 227
  assigning to a domain 61
  Auto Sort 237
  basic information 217
  changing 237
  changing multiple records 238
  committing changes 239
  configuring media channels for 223
  creating. 216

definition . . . 26
deleting . . . 239
employee information . . . 218
entering contact information . . . 218
entering membership information . . . 222
entering system information . . . 220
home directory . . . 291
including in UAD or Avaya Agent Web Client Address Book . . . 221
listing in the Agent Manager . . . 215
out of office . . . 221
overview . . . 214
searching for . . . 236
security information . . . 226
shared directory for . . . 295, 297
shared resources for . . . 298
skills . . . 231
sort listings . . . 237
specifying codes for . . . 308-315
specifying external . . . 221
viewing DataWake for . . . 350
viewing record history . . . 223
workgroups of . . . 240
working directory . . . 292
Agents directory . . . 297
Alarm Monitor . . . 45
Alarm server
about . . . 428
configuration parameters . . . 428
defined . . . 64
re-establishing monitoring . . . 45
alarms . . . 45, 46
filter duplicate . . . 46
alias name for a server . . . 68
analyze flow . . . 483
answered status . . . 99
application.properties file . . . 296, 299
default parameters in . . . 299
WebACD server parameters in . . . 301
approval process
approval queue . . . 131
approval workgroup . . . 130
setting up . . . 129
assigning
agent group memberships . . . 222
agents to domains . . . 61
queues to workgroups . . . 381
servers to domains . . . 55
tenant and workgroup properties . . . 248
associating samples with topic nodes . . . 177
Attribute server
about . . . 432
configuration parameters . . . 432
defined . . . 64
failover information . . . 55
ICM bridge . . . 433
audio visual notification, chat channel . . . 315
auto agent, specifying . . . 220
Auto Load
for agents . . . 215
for servers . . . 62
auto response loop . . . 106
Auto Sort . . . 63, 378
Automatic update option . . . 62
autoresponse loop detection template example . . . 105
autoresponse templates . . . 100
autoresponse threshold . . . 106
Autostart, for servers . . . 69
auxiliary groups . . . 313
auxwork codes . . . 308-315
creating . . . 313
available topics, viewing in FAQ database . . . 324
Avaya Agent
home directory . . . 291
resetting system time zone . . . 46
Avaya Agent Web Client
working directory . . . 292
Avaya IC
determining structure . . . 27
implementing structure . . . 29
overview . . . 26
Avaya IC Customer HTML Chat Client . . . 252
customization . . . 254
customizing . . . 256
features . . . 253
limitations . . . 255
localization . . . 283
software . . . 255
troubleshooting . . . 286
Avaya Interaction Center. *See* Avaya IC
avoid auto response loop . . . 106

B

Backing_Up_And_Restoring_Server_Configuration_Information . . . 38
backup the directory server . . . 38
beep on alarm . . . 46
Blender server
about . . . 434
configuration parameters . . . 434
defined . . . 64
bold . . . 109
bounced message email address . . . 124
browser, environment setting . . . 43
browsers
customers . . . 256
Business Advocate
voice parking device for . . . 376

C

CAAdmin server
- about . . . 438
- configuration parameters . . . 438
- defined . . . 64

Cache button . . . 73
CAServer
- defined . . . 64

categories
- for skills . . . 231
- for wrap up . . . 310

category codes . . . 308-315
changes
- committing . . . 239
- viewing for agent records . . . 223

changing
- agents . . . 237
- configuration records . . . 138
- email format . . . 108
- multiple agent records . . . 238
- privileges . . . 229
- properties . . . 372
- property names and datatypes . . . 372
- property sections . . . 372
- property settings . . . 373
- property values . . . 373
- queues . . . 385
- tables . . . 390
- the Admin password . . . 38

channels
- servers . 420, 428, 432, 434, 438, 440, 453, 477, 482, 488, 502, 504, 554, 556

chat
- Avaya IC Customer HTML Chat Client . . . 252

chat channel
- agent confirmation . . . 302
- configuring for agents . . . 224
- configuring RONA . . . 301
- default timeout . . . 303, 306
- properties for . . . 572
- property for contact arrival . . . 590
- property for enabling . . . 573
- RONA . . . 301
- system properties . . . 644

chat logs, viewing historical . . . 87
chat queue . . . 376
Chat table folder . . . 139
checking for email, overriding default . . . 116
Chinese characters, entering . . . 175
CIRS
- alarm if not found . . . 46
- properties table . . . 139

clearing alarms . . . 45
Clerk role . . . 229
client login flow . . . 436
cluster
- definition . . . 27

codes . . . 308-315
- administration tasks . . . 309
- wrap up codes . . . 310

codes for special characters . . . 566
Codes Manager . . . 308
columns
- sorting and resizing . . . 32

ComHub server
- configuration parameters . . . 443
- defined . . . 64
- domain information . . . 74

commands
- newcall . . . 534

Commit option for servers . . . 79
concurrent administration . . . 55, 56, 74, 79
configuration files for Web Agent . . . 299
Configuration form . . . 208
configuration parameters . . . 418-??
configuration settings, saving . . . 37
Configuration tab . . . 70, 136
- adding new records . . . 137
- default properties . . . 138-151
- deleting records . . . 138
- editing records . . . 138

configuring
- ADU server . . . 420
- agent confirmation . . . 302
- Alarm server . . . 428
- Attribute server . . . 432
- Blender server . . . 434
- CAAdmin server . . . 438
- Content Analyzer server . . . 440
- default timeout . . . 303, 306
- Directory server . . . 453
- Email server . . . 482
- home directory . . . 291
- HTTPVOX server . . . 477
- Java Application Bridge server . . . 488
- Log Collector server . . . 488
- Paging server . . . 502
- Poller server . . . 504
- RONA for chat . . . 301
- servers . . . 70
- UNC to UNIX path mapping . . . 293
- voice queues . . . 382
- WebServices server . . . 554
- Workflow server . . . 556
- working directory . . . 292

configuring, audio notifications for chat . . . 316
configuring, visual notifications for chat . . . 316
configuring,blind chat transfer . . . 281
connections . . . 41

contact acceptance RONA 301, 305
Contact Explorer focus
about 199
Contact form 200
Customer form 202
Queue form 202
using. 200
Contact form. 200
Contact group 201
contact information for agents 218
contact/agentdesktop properties 631
contacts
handled by an agent 203
retrieving by answer time 203
retrieving by date 203
retrieving by wrap up code 203
retrieving for a customer 202
viewing details of 200
container 201
Content Analyzer
basic interface 171
overview 170
samples 176
setting up 171
task privileges 230
topic trees 173
Content Analyzer server
about 440
configuration parameters 440
Control+click 33
copy sample sets 191
copying
codes 309
servers. 79
topic nodes. 175
count, of log files. 71
creating
a list of samples 178
a sample database 177
agent skills 231
agents 216
approval queue. 131
auxwork and logout codes. 313
customer accounts 335
email template folders. 96
Knowledge Bases 182
new configuration records 137
privileges. 229
properties 369, 370
property sections 370
queues. 378
sample sets 180
sample sets from existing sets. 193
servers. 74
sites 37
tables. 388
templates 93
tenants and workgroups 245
topic trees 174
virtual queues 384
wrap up codes 311
creation rules
creating. 210
modifying 208
Creation Rules group 208
creationrules table 204, 206, 208
cumulative inheritance 365
Customer form 202
customer requirements, browsers 256
customer service representative. See agent
customers
creating accounts for 334
default account management process 337
disabling accounts. 337
email address used when sending email from website 322
modifying accounts 335
retrieving contacts for 202
viewing contacts for 200
viewing DataWake history 350
customizing
IC Manager 33
IC Repository 207
tenant website properties 256
tenant websites 329
user information for tenants 332
Web Agent 299
website source code. 331
customizing, popped out chat tab window 318

D

Data Connector server
connecting to 41
defined 64
Data server
configuration parameters. 445
data sources 41
primary 41
secondary 41
database
accessing FAQ 321
connecting to 41
deleting agents from. 239
maintaining FAQ 320
mapping information for IC Repository 199
retrieving records from IC Repository 202
updating agent information. 239
viewing FAQ 321
database connections. 41

Database purge for SQL database 406
Database purge, CCQ database for SQL database. . 410
Database purge, CCQ tables for Oracle database . . 415
Database purge, guidelines for Oracle database . . . 411
Database purge, guidelines for SQL. 406
Database purge, high-level steps for Oracle database 413
Database purge, high-level steps for SQL database . 408
Database purge, IC Repository database for SQL database 409
Database purge, IC Repository tables for Oracle database 414
Database purge, Oracle 411
Database purge, overview for Oracle database . . . 411
Database purge, overview for SQL database 407
datatype, changing for a property 372
DataWake 64, 76, 83, 405, 432, 433
adding filters 346
overview 341
regular expressions 342
ripple regular expressions 342
DataWake, viewing 350
Date macro 104
DCO server
dcobridge account 235
dcobridge account 235
debug levels
for ComHub server 445
for IC Email server 485
for servers 70
for WebACD server 550
setting for IC Manager 42
Debug tab 70
default admin account 29
DefaultTenant 242, 245
definition
agent 214
Avaya IC terms 26
context for website 331
failover 52
FAQ (Web Self-Service) database 320
IC Manager main window 31
precision score 186
properties 241
recall score 186
sample set 177
tenant 241
tenant website 326
virtual queue 384
workgroup 240
DeleteCustomer workflow 338
deleting
agents 239
configuration records 138
email templates. 95
privileges. 229
properties 374
queues 386
sample sets 195
samples 195
servers 79
tables. 389
tenants and workgroups 251
topic nodes 176
user properties 334
device
approval queue 131
definition of 26
using as an agent 214, 221
Device Editor, described 379
Device Manager 377
device. See queues
directory
changing server information in 67
home 291
updating server information 79
working 292
Directory Server
properties for 144
Directory server
about 453
backing up 38
configuration parameters. 453
defined 65
delaying updates to 81
synchronizing multiple 80
tables in 388
displaying inheritance information 249
document
replacing in FAQ database 324
searching for in FAQ database 324
viewing proposed in FAQ database 323
domain
adding servers to 55
assigning agents to 61, 222
creating. 54
definition 26
deleting servers from 55
monitoring alarms 45
overview 52
server failover 56
setting for a server. 68
setting up 53
domain information 74
Domain Manager screenshot 53
DS tables. See tables
DUStore server
configuration parameters. 458
defined 65
dwsensor plugin 83

E

EAI Email server
configuration parameters . . . 460
EAI server
configuration parameters . . . 460
defined . . . 65
EAI Workflow server
configuration parameters . . . 460
Edit Server window, described . . . 67
Editor role . . . 230
EDU server
configuration parameters . . . 460
defined . . . 65
email
changing format . . . 108
formatting . . . 107
formatting text . . . 109
HTML . . . 107, 108
email accounts . . . 111
adding . . . 111
bounced messages . . . 124
overriding default check time . . . 116
testing . . . 117
email activation RONA . . . 305
email address
associated with FAQ document . . . 322
specifying for an agent . . . 218
email channel
configuring for agents . . . 224
properties for . . . 572, 632
property for contact arrival . . . 590
property for enabling . . . 573
RONA . . . 304
system properties . . . 644
email filters . . . 123
email formats
HTML . . . 107
plain text . . . 107
Email Management
approval process . . . 129
auto response loop avoidance . . . 106
email properties . . . 632
email queue . . . 376
Email server
about . . . 482
configuration parameters . . . 482
defined . . . 65
email services . . . 90
task privileges . . . 230
email template administration . . . 90-106
email/agent properties . . . 632
email/runtime properties . . . 632
employee Id, specifying . . . 218
enabling media channels . . . 573
ENV field . . . 74
environment information, setting . . . 43
escalations, and the support role . . . 230
Event collector bridge
defined . . . 65
Event Collector server
configuration parameters . . . 469
defined . . . 65
EventCollector server
configuration parameters . . . 469
EventCollectorBridge server
configuration parameters . . . 472
exact match, from address search . . . 127
examining
sample sets . . . 193
existing sample sets, using as the basis for a new set 193
exiting IC Manager . . . 35
export configuration, environment setting . . . 44
exporting server settings . . . 44
exporting table information . . . 391
expressions
regular . . . 342
ripple regular . . . 342
external agent, specifying . . . 221

F

failover . . . 56
and agents . . . 222
defined . . . 52
domains that do not failover . . . 55
specifying for an individual server . . . 73
FAQ
accessing database . . . 321
editing and deleting topics . . . 324
email address associated with . . . 322
maintaining . . . 320
related topics . . . 320
searching for documents . . . 324
setting up . . . 320
submitting new documents . . . 322
viewing . . . 321
viewing proposed documents . . . 323
FAQ database . . . 82
FAQ database, task privileges for . . . 229
fax number, specifying for an agent . . . 218
field expressions
creating . . . 210
functions for . . . 210
modifying . . . 208
Field Expressions group . . . 209
fieldexpressions table . . . 204, 206, 208
file attachments with templates . . . 104
files, sharing among agents . . . 295, 297

filter duplicates, for alarms . . . 46
Filter tab for email accounts . . . 116
filters for DataWake . . . 346
finding agents . . . 236
focuses in Report Wizard . . . 199
folders, for email templates . . . 96
font
  formats . . . 109
footers in email templates . . . 91
form
  Configuration . . . 208
  Contact . . . 200
  Customer . . . 202
  Queue . . . 202
formats
  changing . . . 108
formatting
  email . . . 107
  email messages . . . 108
frames, described . . . 32

G

General tab
  for email accounts . . . 112
  for servers . . . 68
GlobalPreferences.xml file . . . 296
GlobalResources.xml file . . . 297
group
  Contact . . . 201
  Creation Rules . . . 208
  Customer . . . 202
  Field Expressions . . . 209
  Media Interaction . . . 201
  Queue . . . 202
  Routing Event . . . 201
  Task Performed . . . 201
grouping rules for workgroups . . . 245

H

headers in email templates . . . 91
Heap button . . . 73
help, accessing online . . . 35
historical chat logs . . . 87
history, viewing DataWake records . . . 350
home directory . . . 291
  set up . . . 288
HomeDir property . . . 295, 299
hostname resolution . . . 43
hosts option for alarms . . . 45
HTML email
  about . . . 107
  changing format . . . 108
  formatting . . . 108
  text formats . . . 109
HTML, formats . . . 107
HTTP Connector server
  defined . . . 65
HTTPConnector Server
  properties for . . . 145
HTTPConnector server
  configuration parameters . . . 473
HTTPVOX server
  about . . . 477
Hummingbird SearchServer. See SearchServer

I

IC Email server
  domain information . . . 74
IC Manager
  Admin account . . . 235
  administering to the FAQ database . . . 321
  customizing . . . 33
  exiting . . . 35
  locking . . . 35
  overview . . . 31
  privileges in . . . 229
  resetting system time zone . . . 46
  running multiple versions . . . 36
  using . . . 29
IC Repository
  customizing and mapping . . . 207
  retrieving records from . . . 202
  saving data in . . . 198
icadmin utility . . . 78
ICM Bridge
  enable . . . 433
ICM server
  ICM bridge . . . 433
  icmbridge account . . . 235
ICM service
  properties for . . . 140
  viewing status of . . . 86
icmbridge account . . . 235
ignore low priority alarms . . . 46
import configuration, environment setting . . . 44
importing server settings . . . 44
importing table information . . . 391
incoming email server, specifying . . . 114
inheritance
  displaying information for . . . 249
  for properties . . . 230
  properties . . . 365
  sample scheme for . . . 367
initialization flow . . . 436
Interaction Center. *See* Avaya IC
IPGateway table . . . 146
italic . . . 109

J

Japanese characters, entering . . . 175
Java Application Bridge server
  about . . . 488
JavaAppBridge server
  defined . . . 65

K

keywords for topics . . . 175
Knowledge Bases
  creating . . . 182
  interpreting training results . . . 184
  interpreting validation results . . . 187
  maintaining . . . 190
  putting into production . . . 189
  synchronizing . . . 192
  training . . . 183
  validating . . . 185
  working with . . . 182
Korean characters, entering . . . 175

L

languages
  for codes . . . 309
  for tenant websites . . . 327
lexicons . . . 297
License server
  configuration parameters . . . 493
  defined . . . 66
localization
  Avaya IC Customer HTML Chat Client . . . 283
locking IC Manager . . . 35
Log Collector server
  about . . . 488
log files
  count for . . . 71
  directory for Web Agent . . . 297
  of past chats . . . 87
  size for . . . 71
log levels
  for ComHub server . . . 445
  for IC Email server . . . 485
  for IC Manager . . . 42
  for servers . . . 70
  for WebACD server . . . 550
logging in to IC Manager . . . 29
logon ID, assigning to an agent . . . 220
logout codes, creating . . . 313
lookup tables. See tables

M

macro-average precision . . . 187
macro-average recall . . . 187
macros for templates . . . 102
main window, components of . . . 31
maintaining
  Knowledge Bases . . . 190
  sample associations . . . 191
maintaining a FAQ database . . . 320
management process for customer accounts . . . 337
manager, assigning to an agent . . . 218
Mapping Administration focus
  about . . . 199
  Configuration form . . . 208
mapping specification, for the Report Wizard . . . 206
media channels
  chat configuration . . . 224
  configuration parameters . . . 226
  configuring for agents . . . 223
  email channel properties . . . 632
  email configuration . . . 224
  properties contact arrival . . . 590
  properties enabling . . . 573
  properties for . . . 572
  queues for . . . 376
  system properties . . . 644
  task privileges for email . . . 230
  voice channel properties . . . 646
  voice configuration . . . 225
Media Interaction group . . . 201
Membership tab, described . . . 246
menu bar, described . . . 31
message response templates . . . 91
message template example . . . 105
Messagestatus macro . . . 104
micro-average precision . . . 187
micro-average recall . . . 187
Miscellaneous tab for email accounts . . . 116
Miscellaneous tab on Agent Editor . . . 234
monitoring alarms . . . 45
moving topic nodes . . . 175
multiple agent records, changing . . . 238
multiple items, selecting . . . 33
multiple servers in a domain . . . 54

N

name, specifying for agents . . . 218
names, reserved table names . . . 392
network activity . . . 32
Network button . . . 73
new documents for FAQ database . . . 322
newcall . . . 534

non-cumulative inheritance 366
notes, entering for agents 223
Notification server
defined 66
polling 499

O

online help, accessing 35
Operator role 230
ORB server
adding secondary 75
configuration parameters 500
defined 66
starting 78
out of office, specifying for agents 221
outbound email flow 483
outcome codes 308-315
outcome, for wrap up 310
outgoing email server, specifying 113
overview 26, 242
agent roles 227
agents 214
Content Analyzer 170
email template administration 90
FAQ (Web Self-Service) database 320
IC Manager 31
properties 241, 364
queues and devices 376
servers 64
tables 388
tenants 241
Web Management 81
workgroup 240

P

page push 260
Paging server
about 502
defined 66
parent directory, changing for the Directory server . . 81
parking device, for advocate 376
password
assigning to agents 227
authentication for email accounts 114
authentication for email accounts, SMTP authentication
outgoing emails 113
changing for Admin account 38
performance, improving 62
ping interval, for log files 71
Poller server
about 504
configuration parameters 504, 510
polling for the Notification server 499
Poolname 104
pop up on emergencies 46
POP3 server
specifying account name 112
specifying connection information 112, 114
Postmaster role 230
precision score 186
primary data sources 41
privileges, assigning to agents 227
properties 364-375
agent
home directory 291
working directory 292
assigning to agents 230
assigning to Avaya IC entities 371
assigning to tenants and workgroups 248
changing 372
changing property names and datatypes 372
changing property sections 372
changing settings 373
changing values 373
codes 308-315
configuring for media channels 226
creating 370
creating sections 370
cumulative inheritance 365
definition 26
deleting 374
displaying inheritance information 249
for customer accounts 332
for customizing Web Agent 299
for servers 69
for shared resources 295
for tenant websites 330
inheritance 365
non-cumulative inheritance 366
overview 241, 364
sample inheritance scheme 367
setting up 369
WrapUpEnabled 310
Properties tab, described 246
property
account.text.userprop 333
sametime.server.address 332
security.usercreation 334
userprop.opt.title 334
property descriptions 570-648
admin section 570
admin/agent section 570
admin/agent/channel section 572
admin/general section 573
admin/server section 573
agent section 575
agent/desktop section 577
agent/desktop/AddressBook section 586

Agent/Desktop/Chat 587
Agent/Desktop/Chat/Application 588
agent/desktop/contactsuspension section 590
Agent/Desktop/CustomerContacts 591
agent/desktop/directory section 592
agent/desktop/directory/skillproficiency section . . 595
agent/desktop/directory/voice section 596
agent/desktop/email section 597
agent/desktop/email/alertinfo/req section 599
agent/desktop/email/alertinfo/sme section 600
Agent/Desktop/Email/Application 601
agent/desktop/prompter section 605
Agent/Desktop/QuickFind 606
Agent/Desktop/Resources. 606
agent/desktop/screenpop section 607
agent/desktop/Softphone properties 611
agent/desktop/softphone section. 611
Agent/Desktop/Spelling 612
Agent/Desktop/StatusBar 615
Agent/Desktop/Voice 617
agent/desktop/wac section 622
Agent/Desktop/WebClient 624
Agent/Desktop/WebClient/Connection 627
Agent/Desktop/WebClient/Preferences. 628
Agent/Desktop/WebClient/Preferences/
PreferredWorkload 628
agent/desktop/wrapup 629
agent/desktop/wrapupdialog section 630
agent/security section. 609
contact/agentdesktop section 631
email section 632
email/agent section 632
email/runtime section 632
qui section 633
qui/general section 633
system section 644
voice section 646
property sections
changing 372
creating 370
deleting 374
setting up 369

Q

queue
approval 131
Queue field on Agent Editor 225
Queue form 202
Queue group 202
queues
assigning to workgroups 381
changing 385
creating 378
deleting 386
general information 379
overview 376
types of. 376
viewing usage of 200
virtual. 384
workgroups of. 240
qui properties 633
qui/general properties. 633

R

raise emergency alarms. 46
reason codes. 308-315
reason, for wrap up 310
recall score. 186
refresh
domains 55, 56
servers 74, 79
regular expressions. 342
rejection template. 91
example of 106
related topics in FAQ database 320
re-monitor option for alarms 45
Reply template 104
Report server
configuration parameters. 510
defined 66
specifying data collected by 204
using to save data 198
Report Wizard
about 198
core tables 204
focuses in. 199
mapping specification 206
reference tables 205
using 198
requirements
agent group memberships 222
browsers 256
domains for agents 214
for tenants 241
for workgroups 242
resizing columns 32
Resource Manager
defined 66
Resource Manager server
configuration parameters. 513
ResourceManager server
configuration parameters. 513
resources, sharing among agents 298
restoring the directory server 40
right-click menus 32
ripple regular expressions. 342
role
Administrator 229

Agent . . . 230
Clerk . . . 229
Editor . . . 230
Operator . . . 230
overview . . . 227
Postmaster . . . 230
Supervisor . . . 229
Support . . . 230
RONA
changing default behavior . . . 304, 308
chat channel . . . 301
configuring agent confirmation . . . 302
configuring default timeout . . . 303, 306
configuring for chat . . . 301
contact acceptance . . . 301, 305
email activation . . . 305
email channel . . . 304
ronaenqueueworkgroup_chat . . . 304
ronaenqueueworkgroup_email . . . 308
Routing Event group . . . 201
RoutingHint table . . . 151
running multiple versions of IC Manager . . . 36

S

sametime.server.address tenant property . . . 332
sample associations, maintaining . . . 191
sample database, maintaining . . . 193
sample sets
associating with topics . . . 180
creating from existing . . . 193
definition . . . 177
examining . . . 193
for training . . . 184
removing . . . 195
samples
creating a list of . . . 178
creating individual . . . 181
in Content Analyzer . . . 176
maintaining . . . 193
removing . . . 195
search criteria . . . 178
tagging . . . 177
saving configuration settings . . . 37
sc.xml file . . . 44
searching
for agents . . . 236
for FAQ documents . . . 324
secondary data sources, connections to . . . 41
security
administrator privilege and . . . 227
assigning passwords . . . 227
for agents . . . 226
for servers . . . 69
password authentication . . . 114, 115
security.usercreation tenant property . . . 334
selecting multiple items . . . 33
self-help. See FAQ
server
alias name . . . 68
Auto Load . . . 62
autostart . . . 69
changing server information . . . 67
configuration parameters . . . 418-??
configuring . . . 70
copying . . . 79
creating . . . 74
definition . . . 26
deleting . . . 79
failover for an individual server . . . 73
groups for failover . . . 73
heap, cache and network . . . 73
importing and exporting settings . . . 44
multiple servers in a domain . . . 54
overview . . . 64
properties . . . 69
security for . . . 69
Server Manager . . . 62
sorting . . . 63, 378
starting and stopping . . . 75, 78
status of . . . 73
synchronizing Directory servers . . . 80
updating the directory . . . 79
where hosted . . . 52
Server Manager . . . 62
Server tab for email accounts . . . 112, 114
servers
ADU . . . 420
Alarm . . . 428
Attribute . . . 432
before configuring . . . 419
Blender . . . 434
CAAdmin . . . 438
Content Analyzer . . . 440
Directory . . . 453
Email . . . 482
HTTPVOX . . . 477
ICM . . . 433
Java Application Bridge . . . 488
Log Collector . . . 488
Paging . . . 502
Poller . . . 504
WebServices . . . 554
Workflow . . . 556
set password, for Admin . . . 38
set up
home directory and working directory . . . 288
setting up
agents . . . 216
approval workgroup . . . 130

auto response loop avoidance 106
Avaya IC 29
Content Analyzer 171
database connections 41
domains 53
environment information 43
FAQ database 320
media channels 223
properties and property sections 369
servers 74
sites 37
Web Management servers 81
settings for properties 373
shared directory for agent files 295, 297
shared resources for agent files 298
Shift+click 33
Siebel AED server
configuration parameters 515
Siebel Agent server
defined 66
Siebel AICD server
configuration parameters 515
defined 66
Siebel ASIS server
configuration parameters 515
Siebel EAI server
defined 66
site
assigning agents to 223
creating 37
definition 26
size, of log files 71
skills
assigning to agents 232
creating categories 231
defining 231
sorting
agent information 215
agents 237
codes 309
columns 32
server information 63, 378
special characters
codes for 566
typing 175
starting the ORB server 78
start-up performance, improving 62
status
applying autoresponse template 100
associating with templates 101
for email templates 98, 99
of ICM service 86
of Knowledge Base training 185
of WebACD server 83
status bar, described 32
Status icon 62
status of servers 73
status template 91
example 105
structure of Avaya IC 27
implementing 29
Supervisor Control menu 321
Supervisor role 229
Support role 230
switch password 225
synchronizing a Knowledge Base 192
system information
setting for agents 220
system properties 644
system time zone, resetting 46

T

tables
changing table information 390
creating 388
deleting 389
importing and exporting information 391
overview 388
reserved names 392
tabs, described 32
tagging samples 177
task ceiling
for chat tasks 224
for email tasks 225
for voice tasks 226
setting maximum 221
task levels, specifying for agents 220
task load
for chat tasks 224
for email tasks 224
for voice tasks 225
setting maximum 221
Task Performed group 201
task.autoaccept.time 303, 306
tasks
privileges for 227
Telephony server
configuration parameters 515
Telephony Services Adapter (TSA) server
defined 67
Telephony table folder 145
template macros 102
Template/Status tab 93
templates
associating status with 101
associating with email accounts 115
autoresponse 100
creating 93
for email messages 90-106

modifying . . . 94
samples . . . 105
statuses for . . . 98, 99
Templates tab for email accounts . . . 115
tenant website properties . . . 256
tenants
and workgroups . . . 240
assigning properties . . . 248
assigning queues to . . . 381
creating . . . 245
customizing user information . . . 332
customizing websites for . . . 329
definition . . . 27
deleting . . . 251
language options for . . . 327
modifying . . . 250
overview . . . 241
websites for . . . 326-351
testing
alarms . . . 46
email accounts . . . 117
text
formats . . . 109
threshold, autoresponse . . . 106
Time macro . . . 104
timer environment setting . . . 43
toolbar
adding buttons to . . . 33
described . . . 31
topic trees
copying nodes . . . 175
creating . . . 174
designing . . . 173
tagging samples . . . 177
updating . . . 190
topics
associating with sample sets . . . 180
working with . . . 175
trace levels, for log files . . . 71
Trackingnumber macro . . . 104
training a Knowledge Base . . . 183
training results, interpreting . . . 184
transcripts . . . 87
troubleshooting
Avaya IC Customer HTML Chat Client . . . 286
Debug tab . . . 70
TS server
defined . . . 66
TS.IncomingCall . . . 562
TSA server
configuration parameters . . . 528
TsGroup table . . . 146
TSQS server
configuration parameters . . . 526
defined . . . 67
typing special characters . . . 175, 566

U

UAD or Avaya Agent Web Client Address Book, including agent in . . . 221
UAD or Avaya Agent Web Client Address Book, including agents in . . . 221
UNC to UNIX path mapping
configuring . . . 293
UndeleteCustomer workflow . . . 339
underline . . . 109
update lag . . . 81
UpdateCustomer workflow . . . 338
updating
server information . . . 79
status of a server . . . 62
the Directory server, timing of . . . 81
topic trees . . . 190
URL for tenant website index page . . . 332
userprop.opt.title tenant property . . . 334
users
adding properties to . . . 333
customizing information for . . . 332

V

validating
a Knowledge Base . . . 185
interpreting results . . . 187
with precision and recall scores . . . 188
values
changing for a property . . . 373
deleting for a property . . . 374
values, for properties . . . 370
viewing
DataWake records . . . 350
the FAQ database . . . 321
virtual queue . . . 376, 384
VMM table . . . 147
voice channel
configuring for agents . . . 225
properties for . . . 572, 646
property for contact arrival . . . 590
property for enabling . . . 573
system properties . . . 644
Voice Chat table folder . . . 146
voice parking device . . . 376
voice properties . . . 646
voice queue . . . 376
configuration options . . . 382
VoiceChat table . . . 151
VOX server
configuration parameters . . . 531
defined . . . 67

Vox server
configuration parameters 531
VOX.newcall. 534

W

WACD server configuration tab, ewtAhtSeed 548
WACD server configuration tab, ewtFlavour 548
Web Advocate Adapter (WAA) server
defined. 67
Web Agent
customizing 299
shared files for 296
Web Management
overview 81
server list 83
website account 235
Web Scheduled Callback server
defined. 67
Web Self-Service feature. See FAQ database
WebACD server
configuration parameters 542
configuration parameters for. 301
defined. 67
domain information 74
failover information 55
ronaenqueueworkgroup_chat 304
ronaenqueueworkgroup_email. 308
viewing status 83
WebAdmin plugin 83
WebAdvocateAdaptor server
configuration parameters 540
WebLink 83
WebLM server. 494
WebSchedule Callback. 339
configuring properties 339
WebScheduleCalllback server
configuration parameters 550
WebServices server
about 554
Website
account 235
website account 235
website context 331
Website table folder 148
websites for tenants 326-351
customizing 329
customizing source code 331
language options for 327
specifying index page URL 332
Windows IME 175
workflow
AddCustomer. 337
DeleteCustomer 338
UndeleteCustomer 339
UpdateCustomer 338
Workflow server
about 556
Channels tab 560
configuration parameters. 556
defined 67
failover information 55
WorkFlow table folder. 150
workgroup
approval 130
definition 27
workgroups 242
assigning agents to 222
assigning properties 248
creating. 245
deleting. 251
example 244
grouping rules. 245
modifying 250
overview 240, 242
working directory 292
set up 288
wrap up code, retrieving contacts by 203
wrap up codes 308-315
creating. 311
WrapUpEnabled property 310