Avaya Aura® Contact Center Server Administration

Release 7.0.3
Issue 06.05
July 2018

© 2015-2018, 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 AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

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

License type(s)

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, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

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.

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.

Avaya, the Avaya logo, Avaya one-X® Portal, Avaya Aura® Communication Manager, Avaya Aura® Experience Portal, Avaya Aura® Orchestration Designer, Avaya Aura® Session Manager, Avaya Aura® System Manager, and Application Enablement Services are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction 21
Purpose 21
Intended audience 21
Related resources 21
Avaya Aura® Contact Center Documentation 21
Viewing Avaya Mentor videos 25
Support 26
Chapter 2: Changes in this release 27
Features 27
Ability to run Avaya one-X® Communicator concurrently with Avaya Agent Desktop 28
Ability to store email attachments in the database 28
Agent Desktop integration with Enterprise Web Chat 28
Contact Center database encryption 29
Contact Center services secured by default 29
Database Integration Wizard configuration moved to Contact Center database 29
Database restore not required for reinstating Mission Critical High Availability 30
Data Management - customer privacy 30
File extension restrictions for attachments 30
Increased CCMM customer contact ratio 30
Instant Messaging feature supports Microsoft Skype for Business 2015 31
Interoperation with Avaya Context Store Snap-in using HDX 31
Modify chat transcripts of Enterprise Web Chat 31
Multimedia account passwords must meet minimum complexity criteria 31
Offline Security Store 32
Provision of adding a friendly name for a web chat agent 32
Removal of the default Agent Desktop Dashboard password 32
REST API Enhancements 32
REST API integration 33
Security Manager support for chained certifcates 33
Server Message Block signing enabled on Windows Server 2012 33
Supervisors can change prompts with new Announcement Recorder 33
Whisper Coaching 33
Other changes 34
Automated backup of new security store 34
Avaya Media Server changes 34
Contact Center implements Transport Layer Security version 1.2 by default 35
iceAdmin Windows account privileges reduced 36
Part 1: Contact Center Manager Server 37
Chapter 3: Contact Center Manager Server fundamentals 38

Host Application Integration service functionality 38
HAI service integration with HDX 38
Configuring the HAI service in the Database Integration Wizard 39
Interaction with application commands 40
Stored procedures 42
Feature report 43
Multicast Address and Port Configuration 43
Multicast Stream Control 43
Network Configuration utility 44
Server configuration 44
Web services 45
Chapter 4: Contact Center Manager Server configuration 46
Prerequisites to Contact Center Manager Server configuration 46
Starting the Network Configuration utility 46
Changing the local settings configuration 47
Changing the licensed features configuration 48
Changing the Avaya Communication Server 1000 switch data 50
Changing the Voice Services configuration 51
Changing the SIP Local Subscriber data 52
Changing the SIP Network Settings data 54
Enabling support for three Call Appearance lines 56
Chapter 5: Contact Center Manager Server statistics configuration 57
Prerequisites to Contact Center Manager Server statistics configuration 57
Configuring the Multicast controller 57
Changing the IP multicast settings 59
Disconnecting Terminal Services sessions 60
Chapter 6: Database Integration Wizard configuration 62
Prerequisites to Database Integration Wizard configuration 62
Configuring a data source name for a third-party database 63
Configuring the HDX provider ID 64
Configuring TAPI server settings 65
Configuring database connections 66
Configuring Web services 67
Creating statements to access a database using SQL or stored procedures 70
Testing statements that use Web service methods 72
Updating an SQL or stored procedure statement 73
Updating a Web service 74
Deleting an SQL statement or stored procedure 75
Removing a Web service 76
Configuring the Contact Center Manager Server flow application 77
Chapter 7: REST API configuration 79
Adding a new environment 80
Creating and testing REST requests 80

Updating a REST request ... 82
Deleting a REST request ... 82
Updating an environment ... 82
Deleting an environment ... 83
Part 2: Contact Center License Manager ... 84
Chapter 8: Licensing administration ... 85
Resetting the grace period ... 85
Updating the license file ... 86
Changing from Nodal to Corporate licensing ... 87
Changing the licensing information on Contact Center Manager Server ... 88
Refreshing your server ... 89
Configuring remote Avaya WebLM server details ... 89
Part 3: Contact Center Manager Server Utility ... 91
Chapter 9: Server Utility Access Class operations ... 92
Prerequisites to Contact Center Manager Server Utility access class operations ... 92
Logging on to Server Utility ... 92
Creating an access class ... 93
Viewing members of an access class ... 94
Modifying access class properties ... 94
Previewing the list of access classes ... 95
Printing the list of access classes ... 96
Deleting an access class ... 96
Chapter 10: Connected user and user account operations ... 97
Prerequisites to Contact Center Manager Server Utility connected user operations ... 97
Viewing a list of connected users ... 97
Logging off a user ... 98
Setting privileges for a user ... 98
Adding desktop user accounts ... 103
Preventing users from accessing the server ... 104
Restoring access to the server for a user ... 105
Resetting desktop passwords ... 105
Changing the properties of a desktop user ... 106
Deleting a desktop user ... 107
Chapter 11: Serial port configuration ... 108
Prerequisites to Contact Center Manager Server Utility serial port configuration ... 108
Viewing port settings ... 108
Editing port settings ... 109
Chapter 12: Server settings ... 110
Prerequisites to Contact Center Manager Server Utility server settings ... 110
Viewing server resources ... 110
Chapter 13: PABX configuration ... 111
Prerequisites to Contact Center Manager Server Utility PABX configuration ... 111

Recording PABX information 111
Chapter 14: Alarm and Event configuration 112
Prerequisites to Event Browser configuration 113
Starting the Event Browser from Server Utility 113
Sorting events in the Event Browser 113
Viewing online Help for an event 113
Saving a list of events 114
Changing the filtering criteria for events 114
Adding an event preference 115
Throttling all events 116
Changing an event preference 117
Deleting an event preference 118
Changing the classification of an event 118
Opening the Alarm Monitor 118
Refreshing the Alarm Monitor 119
Sorting events in the Alarm Monitor 119
Specifying when the Alarm Monitor appears in the foreground 119
Configuring the Alarm Monitor to appear in the background 120
Obtaining more information about an alarm 120
Manually clearing an alarm 121
Chapter 15: Voice Prompt Editor configuration 122
Prerequisites to Voice Prompt Editor procedures 122
Logging on to the Voice Prompt Editor 122
Logging off the Voice Prompt Editor 123
Creating a voice file 123
Opening a voice file 124
Reverting to a previously saved voice file 124
Copying a voice file 124
Renaming a voice file 125
Deleting a voice file 125
Restoring a voice file 125
Creating a voice segment 126
Recording a voice segment 126
Playing a voice segment 127
Playing a group of voice segments 127
Searching for a voice segment 128
Lengthening or shortening a voice segment 129
Removing all silence from a voice segment 130
Removing or adding a specified length to all voice segments 130
Removing all silence from all voice segments 131
Deleting a voice segment 132
Restoring a voice segment marked for deletion 132
Part 4: Contact Center Manager Administration 133

Chapter 16: Contact Center Manager Administration configuration 134
Prerequisites to Contact Center Manager Administration configuration 134
Configuring your logon warning message title and text 134
Enabling the logon warning message 135
Configuring Real-Time Reporting 136
Configuring Emergency Help 138
Configuring email notifications for Historical reporting 139
Configuring SMTP Server on the Contact Center Manager Administration Server 140
Creating a shared folder to export historical reports 142
Configuring Contact Center Manager Administration security settings 143
Installing the Orchestration Designer 144
Configuring Agent Desktop Displays parameters on the server 145
Changing the password for the iceAdmin user account 147
Configuring the LPR port for printers 149
Configuring a network printer for CCMA 149
Installing the XML Automated Assignments feature 150
Configuring Avaya Call Recording and Quality Monitoring 151
Configuring CDN Landing Pads for Universal Networking or Integrated Reporting 152
Configuring a DNIS Landing Pad for Universal Networking 153
Chapter 17: Avaya Communication Server 1000 Data Extraction Tool operation 155
Prerequisites to Avaya Communication Server 1000 Data Extraction Tool 155
Extracting data from a serial connection 156
Extracting data using a modem 157
Extracting data from a file 158
Capturing Terminal Number data 159
Capturing voice port data 161
Capturing CDN data 161
Capturing IVR ACD-DN data 162
Capturing route data 163
Chapter 18: Language support fundamentals 164
Language levels 166
Language family compatibility 166
Configuring the operating system language 167
Setting the system locale 168
Enabling a localized language 169
Accessing the CCMA Web client using a localized language 169
Part 5: Network Control Center Server 171
Chapter 19: Network Control Center server administration 172
Prerequisites 172
Adding a site to the NCC 172
Deleting a site from the NCC 174
Adding access classes 175

Adding a site in Contact Center Manager Administration 175
Configuring Landing Pads for Universal Networking 177
Configuring network communication parameters 178
Synchronizing site information 180
Adding a network skillset 181
Deleting a network skillset 182
Configuring network skillset properties 182
Configuring Agent Order Preference 183
Configuring the routing tables 184
Configuring routing table assignments 184
Configuring the historical statistics collection 186
Configuring MCDN network CDNs 187
Configuring DNIS Network CDNs 188
Part 6: Communication Control Toolkit 190
Chapter 20: Communication Control Toolkit fundamentals 191
Automatic Call Distribution 191
Communication Control Toolkit Administration Console 191
Communication Control Toolkit Web Administration 192
Trace Control Utility 192
Programming interfaces 192
Communication Control Toolkit Reference Client 193
Chapter 21: Resource bulk management 194
Prerequisites to resource management 194
Importing Windows users 194
Importing Avaya Communication Server 1000 data 196
Importing workstations from the domain 198
Importing bulk resources 199
Exporting bulk resources 200
Part 7: Contact Center Multimedia 203
Chapter 22: Contact Center Multimedia fundamentals 204
Email contact type 205
Email rule groups 206
Recipient mailboxes 206
Inbound email settings 207
Outbound email settings 207
Character encoding for outgoing email messages 207
Asian email 208
Email traffic reports 208
Extended Email Capacity 209
Supervisor approval of email messages 210
Agent Desktop 212
Contact Center Manager Administration 212

Web services 212
Open Interfaces for email 213
CCMM Dashboard utility 215
SMS text messages, faxes, scanned documents, and voice mail attachments 216
Mailbox configuration 217
Traffic reports 217
Agent Desktop 218
Outbound contact type 218
Outbound Campaign Management Tool 218
Campaign Scheduler 219
Agent Desktop 219
Contact Center Manager Administration 220
Web services 220
Web communications 220
Instant Messaging 221
Office hours 221
Contact Center Multimedia in a voice-only solution 222
Chapter 23: General configuration 224
Prerequisites for general configuration 224
Starting the CCMM Administration utility 224
Configuring general settings 225
Configuring the reporting credentials 226
Adding administrators 226
Removing administrators 228
Configuring office hours 228
Configuring holidays 229
Applying office hours 230
Viewing real-time traffic reports by contact 231
Configuring the displayed date for traffic reports 232
Configuring Web On Hold comfort groups for a Web communications skillset 232
Removing a Web On Hold comfort group for a Web communications skillset 233
Configuring Web communications comfort groups for a Web communications skillset 234
Removing a Web communications comfort group from a Web communications skillset 234
Configuring a Geographic Alternative Communication Control Toolkit server 235
Deleting a Geographic Alternate Communication Control Toolkit server 236
Configuring a Reporting Server 236
Configuring a Directory LDAP server 237
Configuring a Phonebook LDAP server 238
Chapter 24: Outbound configuration 240
Prerequisites for Outbound configuration 240
Configuring a route point for an Outbound skillset 240
Chapter 25: Email configuration 242
Prerequisites for email configuration 243

Configuring the email server names ... 243
Adding an email server ... 245
Deleting an email server ... 246
Configuring skillsets for email ... 247
Creating or changing a recipient mailbox ... 247
Creating or changing an alias for a recipient mailbox ... 250
Deleting a recipient mailbox ... 252
Updating the system default rule ... 253
Updating the system delivery failure rule ... 254
Creating or changing a keyword group ... 256
Deleting a keyword from a keyword group ... 257
Deleting a keyword group ... 258
Creating or changing prepared responses ... 258
Deleting prepared responses ... 261
Removing attachments from prepared responses ... 262
Promoting suggested responses ... 262
Creating or changing a sender group ... 263
Deleting a sender group ... 264
Deleting a sender from a sender group ... 265
Creating or changing rules ... 265
Enabling a rule ... 268
Disabling a rule ... 269
Deleting a rule ... 269
Creating or changing rule groups ... 270
Configuring supervisor approval for email messages on a per skillset basis ... 271
Configuring auto-rejection of email messages from all skillsets that use approval hierarchy ... 273
Configuring the email settings ... 274
Changing the character encoding for outgoing and incoming email ... 275
Selecting the outgoing email address ... 276
Barring email addresses ... 277
Deleting a barred email address ... 278
Configuring Microsoft Exchange for sending outgoing email ... 278
Adding a certificate for use with TLS email connections ... 279
Enabling SMTP Authentication on your email server ... 281
Determining if SMTP Authentication is enabled ... 282
Adding an email address of an administrator in CCMM Dashboard ... 283
Enabling Extended Email Capacity ... 284
Disabling Extended Email Capacity ... 285
Configuring Open Interfaces for email ... 285
Disabling email retrieval for all mailboxes ... 288
Reenabling email retrieval for all mailboxes ... 288
Chapter 26: Voice mail configuration ... 290
Prerequisites for voice mail configuration ... 290

Configuring a route point for a voice mail skillset ... 291
Adding a voice mail server ... 291
Updating a voice mail server ... 292
Deleting a voice mail server ... 292
Adding a voice mail mailbox ... 293
Updating a voice mail mailbox ... 295
Deleting a voice mail mailbox ... 295
Updating the voice mail system default rule ... 296
Updating the voice mail system delivery failure rule ... 297
Chapter 27: Scanned document configuration ... 299
Prerequisites for scanned document configuration ... 299
Configuring a route point for a scanned document skillset ... 300
Adding a document imaging server ... 300
Updating a document imaging server ... 301
Deleting a document imaging server ... 301
Adding a scanned document mailbox ... 302
Updating a scanned document mailbox ... 303
Deleting a scanned document mailbox ... 304
Configuring a scanned document reply mailbox ... 304
Deleting a scanned document reply mailbox ... 306
Updating the scanned documents system default rule ... 306
Updating the scanned documents system delivery failure rule ... 307
Chapter 28: Fax configuration ... 309
Prerequisites for fax configuration ... 309
Configuring a route point for a fax skillset ... 309
Adding a fax server ... 310
Updating a fax server ... 311
Deleting a fax server ... 311
Adding a fax mailbox ... 312
Updating a fax mailbox ... 313
Deleting a fax mailbox ... 314
Configuring a fax reply mailbox ... 314
Deleting a fax reply mailbox ... 316
Updating the fax system default rule ... 316
Updating the fax system delivery failure rule ... 317
Chapter 29: Social Network Configuration ... 319
Configuring the Social Networking System Default Rule ... 320
Configuring Social Networking channels ... 321
Adding a new Social Networking language ... 321
Configuring Social Networking mailboxes ... 322
Configuring mailboxes for transferred Social Networking contacts ... 324
Chapter 30: Instant message configuration ... 326
Configuring welcome and disconnect messages ... 326

Creating automatic phrases ... 327
Creating a page push URL ... 328
Adding an expert manually to Contact Center Multimedia ... 328
Importing an expert from files to Contact Center Multimedia ... 329
Adding experts to a skillset ... 330
Creating an expert group ... 330
Chapter 31: Short Message Service configuration ... 332
Prerequisites for SMS configuration ... 332
Configuring a route point for an SMS skillset ... 333
Adding an SMS Gateway ... 333
Updating an SMS Gateway ... 334
Deleting an SMS Gateway ... 334
Adding a SMS mailbox ... 335
Updating an SMS mailbox ... 336
Deleting an SMS mailbox ... 337
Configuring an SMS reply mailbox ... 337
Deleting an SMS reply mailbox ... 339
Updating the SMS system default rule ... 339
Updating the SMS system delivery failure rule ... 340
Chapter 32: Web communications configuration ... 342
Prerequisites for Web communications configuration ... 343
Assigning a development Web server name ... 343
Configuring welcome messages and text chat labels ... 344
Configuring Enterprise Web Chat settings ... 346
Configuring skillsets for Web Communications ... 347
Configuring Web communications agent timers ... 348
Saving Web communications chat session details ... 349
Configuring the Web communications chat session limits ... 350
Configuring customer notification log ... 350
Enabling Web Communications transfer to a skillset ... 351
Creating automatic phrases ... 351
Deleting an automatic phrase ... 352
Creating a page push URL ... 353
Deleting a page push URL ... 354
Creating Web On Hold URLs groups ... 354
Deleting a URL from a Web On Hold URL group ... 355
Deleting a Web On Hold URLs group ... 356
Creating Web On Hold comfort groups ... 356
Deleting a message from a Web On Hold comfort group ... 357
Deleting a Web On Hold comfort group ... 358
Creating Web communications comfort groups ... 358
Changing the sequence of messages in a Web communications comfort group ... 359
Deleting a message from a Web communications comfort group ... 360

Deleting a Web communications comfort group 360
Configuring intrinsics for agent-supervisor observe and barge-in 361
Chapter 33: Agent Desktop configuration 363
Adding a friendly name for a web chat agent 363
Controlling access to email message text 364
Configuring supervisor approval for email messages on a per agent basis 365
Configuring agent access to contacts 365
Disabling the Avaya Agent Desktop embedded softphone 366
Creating or changing custom fields in Agent Desktop 367
Deleting a custom field in Agent Desktop 367
Configuring the active contact timer 368
Configuring the callback timer 368
Configuring the callback trunk access 369
Specifying the attachment size 370
Configuring Agent Desktop behavior 370
Configuring the state of the Agent terminal on log off 371
Configuring hotdesking 371
Configuring hotdesking in a Citrix environment 372
Configuring Web statistics 372
Configuring Web reporting 373
Creating or changing a closed reason 373
Configuring default closed reasons 374
Deleting a closed reason 375
Configuring Shortcut keys for Agent Desktop 375
Configuring Basic Screen Pops 376
Configuring Advanced screen pop applications 380
Configuring Advanced screen pop filters 381
Configuring Advanced Screen pops 382
Enabling Customer History on Voice Contacts 385
Restricting file extensions for attachments 386
Configuring Advanced Settings 387
Configuring Advanced Settings in a voice-only solution 391
Configuring User Settings 394
Configuring User Settings in a voice-only solution 408
Configuring IIS to support MDB database file attachments in email messages 418
Chapter 34: Data Management - cleanup and purging 420
Starting the Multimedia Data Management utility 424
Creating an Outbound Campaigns cleanup rule 425
Creating an Email Rules cleanup rule 426
Creating a Skillsets cleanup rule 426
Creating a Closed Reason cleanup rule 427
Creating a Customers cleanup rule 428
Creating a new scheduled cleanup task 429

Enabling OFFLINE database purging ... 431
Restoring an archive from a previous Release ... 431
Chapter 35: Data Management - customer privacy ... 433
Generating a customer information file ... 433
Deleting customer history ... 434
Part 8: Avaya Aura® Media Server ... 435
Chapter 36: Avaya Aura® Media Server configuration ... 436
Prerequisites to Avaya Aura® Media Server configuration ... 436
Logging on to Avaya Aura® Media Server Element Manager ... 436
Uploading a batch zip file ... 437
Configuring Avaya Aura® Media Server name resolution ... 438
Enabling SNMP traps ... 438
Configuring the Avaya Aura® Media Server SNMP agent ... 440
Configuring log filter settings ... 440
Part 9: Security Administration ... 443
Chapter 37: Security Fundamentals ... 444
Simple Network Management Protocol ... 444
Event viewer settings ... 444
Event Browser and Alarm Monitor ... 445
Contact Center Manager Server Utility to view events on CCMS ... 445
Chapter 38: Contact Center security certificates administration ... 447
Backing up the security store ... 449
Deleting a security store ... 450
Creating a new security store ... 450
Creating a security store with Subject Alternative Names ... 452
Copying the Certificate Signing Request file ... 453
Adding certificate files to the security store ... 454
Exporting a root certificate from the security store ... 456
Applying the root certificate to a Contact Center client ... 456
Creating an offline store ... 457
Switching between the active and offline security stores ... 459
Making an offline store active ... 459
Turning on Web Services security ... 460
Configuring the minimum TLS version ... 461
Configuring SMTP server details ... 462
Scheduling a security store inspection task ... 463
Verifying the scheduled security store inspection task ... 465
Examining a certificate file in the security store ... 465
Removing a certificate file from the security store ... 466
Modifying a scheduled security store inspection task ... 466
Removing a scheduled security store inspection task ... 467
Recreating the CCMA security bindings ... 467

Turning off Web Services security 468
Chapter 39: Database encryption administration 470
Creating and activating an encryption key 471
Encrypting the Contact Center database 472
Decrypting the Contact Center database 472
Chapter 40: Windows Server 2012 security for Contact Center 474
Disabling Server Message Block signing in the server local group policy 474
Chapter 41: Avaya Aura® Media Server security certificates administration 476
Importing the Contact Center root certificate into Avaya Aura® MS 476
Creating a new certificate signing request for Avaya Aura® Media Server 477
Adding signed certificate files to the Avaya Aura® MS key store 478
Assigning a server certificate to an Avaya Aura® MS service profile 479
Exporting a root certificate from Avaya Aura® MS in PKCS12 format 479
Exporting a root certificate from Avaya Aura® MS in PEM format 480
Part 10: Common server administration 482
Chapter 42: Microsoft Windows configuration and management 483
Managing date and time features 483
Disabling the Windows time service 483
Verifying Service Packs 484
Configuring the operating system for remote access 485
Chapter 43: Simple Network Management Protocol administration 486
Configuring Windows SNMP Service 486
Selecting CCMS events to be forwarded 487
Selecting CCMA, LM, CCT, and CCMM events to be forwarded 487
Copying Event to Trap Translator settings from one Contact Center server to another 489
Configuring the NMS 490
Chapter 44: Contact Center server High Availability 491
Prerequisites to Contact Center Server High Availability 492
Configuring hot-standby managed IP address 492
Configuring the hot-standby server 493
Disabling High Availability on a Hot-standby server 494
Configuring the notification of automatic switchovers 495
Configuring hot-standby manual switchovers 496
Configuring service monitoring 497
Configuring hot standby automatic switchovers 499
Monitoring switchover information 500
Reviewing shadowing 501
Configuring campus Mission Critical High Availability on the active server 501
Configuring Mission Critical High Availability on the Standby Server 503
Starting a Mission Critical Active Server 505
Starting shadowing on a Mission Critical Standby Server 506
Stopping High Availability on a Mission Critical Standby Server 506

Stopping High Availability on a Mission Critical Active Server 507
Disabling Auto Startup on a Mission Critical server after reboot 507
Selecting a startup mode on the Mission Critical Standby server after reboot 508
Re-enabling High Availability after stopping services 508
Reinstating Mission Critical High Availability 508
Reinstating Hot Standby High Availability 510
Reinstating High Availability on a Multimedia Contact Server Only 511
How to manually switch over to a Remote Geographic Node 512
How to revert to a campus site after running the RGN 513
How to manually switch over to the Remote Geographic Node in an AML CS1000-based solution 516
How to revert to the campus site after running the RGN for a few days 517
Chapter 45: Common procedures 519
Starting or stopping Contact Center applications 519
Part 11: Server name or IP address change 520
Chapter 46: Server name or IP address change 521
Server name change and security certificates 521
High Availability solution server renaming considerations 522
Prerequisites for changing server names or IP addresses 523
Chapter 47: Voice and Multimedia Contact Server name change 524
Voice and Multimedia Contact Server name change prerequisites 524
Turning off Web Services security 524
Changing the server name in the operating system 525
Verifying the server name change 526
Synchronizing the operating system name with the Voice and Multimedia Contact Server name 526
Configuring the server name details 527
Joining the server to the domain 527
Updating the HOSTS file on the Voice and Multimedia Contact Server 528
Resetting the iceAdmin password 528
Configuring destination for exported scheduled reports 529
Reconfiguring security certificates after changing the server name 530
Changing the server name in the Administration tool 531
Changing the CCT server name in the Administration tool 531
Changing the CCMA and CCMM server name in the Dashboard 532
Changing the CCMM server name in the Administration tool 532
Updating the email attachment folders 533
Configuring the external Web Communications server 533
Updating shared folders for reports 534
Configuring the Contact Center Multimedia settings 535
Updating the HOSTS file for clients 536
Configuring the Agent Desktop 537
Configuring Avaya Aura® Media Server name resolution 537

Chapter 48: Voice and Multimedia Contact Server IP address change 538
Changing the contact center subnet IP address of the Voice and Multimedia Contact Server 538
Configuring the Voice and Multimedia Contact Server IP address 539
Verifying the server IP address change 539
Updating the Network Control Center server 540
Updating the HOSTS file 540
Updating the server IP address in CCMA 541
Updating the HOSTS file for clients 541
Updating shared folders for reports 542
Updating the Communication Control Toolkit server IP address in CCMA 543
Verifying the Communication Control Toolkit provider IP address 544
Updating the Contact Center Multimedia server IP address in CCMA 544
Configuring Avaya Aura® Media Server name resolution 545
Chapter 49: Voice Contact Server name change 546
Prerequisites for Voice Contact Server name change 546
Changing the server name in the operating system 546
Verifying the server name change 547
Synchronizing the operating system name with the Voice Contact Server name 548
Configuring the server name details 548
Joining the server to the domain 549
Updating the HOSTS file on the Voice Contact Server 549
Resetting the iceAdmin password 550
Configuring destination for exported scheduled reports 550
Reconfiguring security certificates after changing the server name 552
Changing the server name in the Administration tool 552
Changing the CCT server name in the Administration tool 553
Changing the CCMA and CCMM server name in the Dashboard 553
Updating the HOSTS file for clients 554
Updating shared folders for reports 555
Configuring the Contact Center Multimedia settings 556
Configuring Avaya Aura® Media Server name resolution 557
Chapter 50: Voice Contact Server IP address change 558
Changing the contact center subnet IP address of the Voice Contact Server 558
Configuring the Voice Contact Server IP address 559
Verifying the server IP address change 559
Updating the Network Control Center server 560
Updating the HOSTS file 560
Updating the server IP address in CCMA 561
Updating the HOSTS file for clients 561
Updating shared folders for reports 562
Updating the Communication Control Toolkit server IP address in CCMA 563
Verifying the Communication Control Toolkit provider IP address 564

Configuring Avaya Aura® Media Server name resolution 564
Chapter 51: Multimedia Contact Server name change 566
Prerequisites for Multimedia Contact Server name change 566
Turning off Web Services security 566
Changing the server name on the operating system 567
Verifying the server name change 568
Synchronizing the operating system name with the Multimedia Contact Server name 568
Joining the server to the domain 569
Updating the HOSTS file on the Multimedia Contact Server 569
Reconfiguring security certificates after changing the server name 570
Changing the CCMA and CCMM server name in the Dashboard 570
Updating the email attachment folders 571
Changing the server name for Enterprise Web Chat 572
Configuring the external Web Communications server 572
Updating the CCMM server information in Contact Center Manager Administration 573
Updating the HOSTS file for clients 574
Configuring the Agent Desktop 574
Chapter 52: Multimedia Contact Server IP address change 576
Changing the IP address on the operating system 576
Verifying the server IP address change 577
Updating the HOSTS file 577
Updating the CCMM server IP address in Contact Center Manager Administration 578
Chapter 53: Avaya Aura® Media Server server name change 579
Changing the name of the Avaya Aura® Media Server on Linux 579
Re-configuring security certificates after changing the Avaya Aura® Media Server server name 580
Updating the standalone Avaya Aura® Media Server name in CCMA 581
Chapter 54: Avaya Aura® Media Server IP address change 582
Changing the Avaya Aura® Media Server IP address on Linux 582
Updating the standalone Avaya Aura® Media Server IP address in CCMA 583
Appendix A: Default login values 585

Chapter 1: Introduction

Purpose

This document contains information about how to perform additional configuration tasks for Avaya Aura® Contact Center, including server maintenance tasks, administrative tasks, managing data, configuring data routing, performing archives, and multimedia configuration. It also describes the optional configuration procedures for server configuration.

Intended audience

This document is intended for people who perform system administration and configuration on the Avaya Aura® Contact Center server.

Related resources

Avaya Aura® Contact Center Documentation

The following table lists the documents related to Avaya Aura® Contact Center. Download the documents from the Avaya Support website at https://support.avaya.com.

Title	Use this document to:	Audience
Overview		
Avaya Aura® Contact Center Overview and Specification	This document contains technical details you need to set up your Contact Center suite. The document contains the background information you need to plan and engineer your system (server preparation information, routing options, licensing configurations, and hardware	Customers and sales, services, and support personnel

Table continues…

Title	Use this document to:	Audience
	configuration). The document also contains background information you require to install all software components that are part of and work with Contact Center. General information about considerations for upgrading your existing suite of Contact Center is also included. This document contains strategies and requirements to plan your network configuration and prepare your servers for Contact Center software installations.	
Avaya Aura® Contact Center and Avaya Aura® Unified Communications Solution Description	This document describes the solution architecture, suggested topologies, and capacities for the Avaya Aura® Unified Communications platform. This document also describes the features and functional limitations of certain configurations.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center and Avaya Communication Server 1000 Solution Description	This document describes the solution architecture, suggested topologies, and capacities for the Avaya Communication Server 1000 platform. This document also describes the features and functional limitations of certain configurations.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center Documentation Catalog	This document describes available Avaya Aura® Contact Center documentation resources and indicates the type of information in each document.	Customers and sales, services, and support personnel
Avaya Aura® Contact Center Terminology	This document contains definitions for the technical terms specific to Contact Center.	Customers and sales, services, and support personnel
Contact Center Performance Management Data Dictionary	This document contains reference tables that describe the statistics and data in the historical and real-time reports generated in Contact Center.	System administrators and contact center supervisors
Implementing		
Avaya Aura® Contact Center and Avaya Aura® Unified Communications Integration	This document contains information and procedures to integrate the Avaya Aura® Unified Communications platform with Contact Center.	Implementation personnel

Table continues…

Title	Use this document to:	Audience
Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration	This document contains information and procedures to integrate the Avaya Communication Server 1000 platform with Contact Center.	Implementation personnel
Deploying Avaya Aura® Contact Center DVD for Avaya Aura® Unified Communications	This document contains information about Contact Center DVD installation, initial configuration, and verification for the Avaya Aura® Unified Communications platform.	Implementation personnel
Deploying Avaya Aura® Contact Center DVD for Avaya Communication Server 1000	This document contains information about Contact Center DVD installation, initial configuration, and verification for the Avaya Communication Server 1000 platform.	Implementation personnel
Deploying Avaya Aura® Contact Center Software Appliance for Avaya Aura® Unified Communications	This document describes how to deploy the Avaya Aura® Contact Center Software Appliance for the Avaya Aura® Unified Communications platform.	Implementation personnel
Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications	This document contains information for Contact Center preparation, process, initial configuration, and verification of the installation on the Avaya Aura® Unified Communications platform.	Implementation personnel
Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000	This document contains information for Contact Center preparation, process, initial configuration, and verification of the installation on the Avaya Communication Server 1000 platform.	Implementation personnel
Avaya Aura® Contact Center and Proactive Outreach Manager Integration	This document provides conceptual and procedural information on the integration between Avaya Aura® Contact Center (AACC) and Avaya Proactive Outreach Manager (POM); it describes the tasks required for AACC and POM integration.	Implementation personnel
Upgrading and patching Avaya Aura® Contact Center	This document contains information and procedures to upgrade from previous releases to Contact Center, migrating the databases, and information and procedures to download and install service packs.	Implementation personnel and system administrators
Administering		
Avaya Aura® Contact Center Server Administration	This document contains information and procedures for day-today	System administrators

Table continues…

Title	Use this document to:	Audience
	maintenance of all servers in the Contact Center suite, including server maintenance tasks, administrative tasks, managing data, configuring data routing, performing archives, and backing up data. It also describes the optional configuration procedures for server configuration.	
Avaya Aura® Contact Center Client Administration	This document contains information and procedures to configure the users and user access, skillsets, server management, and configuration data in the Contact Center database.	System administrators and contact center supervisors
Using Contact Center Orchestration Designer	This document contains information and procedures to configure script and flow applications in Contact Center Orchestration Designer.	System administrators
Maintaining		
Maintaining Avaya Aura® Contact Center	This document contains routine maintenance procedures such as installing service packs, and maintaining the databases for the Contact Center system.	System administrators and support personnel
Troubleshooting Avaya Aura® Contact Center	This document contains system-wide troubleshooting information and procedures for Contact Center hardware, software, and network.	System administrators and support personnel
Contact Center Event Codes	This document contains a list of errors in the Contact Center suite and recommendations to resolve them. This document is a Microsoft Excel spreadsheet.	System administrators and support personnel
Using		
Using Avaya Aura® Contact Center Reports and Displays	This document contains procedures to generate performance reports, and to monitor and analyze performance data and performance measurements.	System administrators and contact center supervisors
Using Agent Desktop for Avaya Aura® Contact Center	This document provides information and procedures for agents who use the Agent Desktop application to accept, manage, and close contacts of all media types in Contact Center.	Contact center agents and supervisors
Using the Contact Center Agent Browser application	This document provides information and procedures for agents who use	Contact center agents

Table continues…

Title	Use this document to:	Audience
	the Agent Browser application to log on to Contact Center and perform basic tasks.	

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- 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: Changes in this release

The following section details what has changed in *Avaya Aura® Contact Center Server Administration* Release 7.0.

- Features on page 27
- Other changes on page 34

Features

New features in the Release 7.0 base build

See the following sections for information about new features in the Release 7.0 base build:

- Contact Center services secured by default on page 29
- Database restore not required for reinstating Mission Critical High Availability on page 30

New features in Release 7.0 Feature Pack 1

See the following sections for information about new features added by Feature Pack 1:

- Ability to run Avaya one-X Communicator concurrently with Avaya Agent Desktop on page 28
- Agent Desktop integration with Enterprise Web Chat on page 28
- Database Integration Wizard configuration moved to Contact Center database on page 29
- File extension restrictions for attachments on page 30
- Instant Messaging feature supports Microsoft Skype for Business 2015 on page 31
- Interoperation with Avaya Context Store Snap-in using HDX on page 31
- Modify chat transcripts of Enterprise Web Chat on page 31
- Multimedia account passwords must meet minimum complexity criteria on page 31
- Provision of adding a friendly name for a web chat agent on page 32
- Removal of the default Agent Desktop Dashboard password on page 32
- Server Message Block signing enabled on Windows Server 2012 on page 33
- Supervisors can change prompts with new Announcement Recorder on page 33
- Whisper Coaching on page 33

New features in Release 7.0 Feature Pack 2

See the following sections for information about new features added by Feature Pack 2:

- Increased CCMM customer contact ratio on page 30
- Offline Security Store on page 32
- REST API integration on page 33

New features in Release 7.0 Feature Pack 3

See the following sections for information about new features added by Feature Pack 3:

- Ability to store email attachments in the database on page 28
- Contact Center database encryption on page 29
- Data Management - customer privacy on page 30
- REST API Enhancements on page 32
- Security Manager support for chained certifcates on page 33

Ability to run Avaya one-X® Communicator concurrently with Avaya Agent Desktop

From Release 7.0 Feature Pack 1, Contact Center administrators can disable the Avaya Agent Desktop embedded softphone either on a per agent basis or on a system-wide basis. When the administrators disable the embedded softphone, Avaya one-X® Communicator can run concurrently with Avaya Agent Desktop.

Ability to store email attachments in the database

From Release 7.0 Feature Pack 3, there is an option to save new email attachments in the MULTIMEDIA database instead of on the file system. You can configure this option using the Multimedia Administration utility.

Agent Desktop integration with Enterprise Web Chat

Agent Desktop Release 7.0 Feature Pack 1 integrates with Enterprise Web Chat (EWC). Agent Desktop Release 7.0 Feature Pack 1 provides two services for web chat: the Web Communications text chat and EWC. Use EWC if you require a large number of web chat sessions. EWC can support up to 3000 simultaneous Web chat sessions.

Agent Desktop integration with EWC is supported only if Avaya Aura® Contact Center is deployed on Communication Manager with a standalone Multimedia server. EWC is a licensed feature. For Agent Desktop to handle EWC contacts, administrators must enable a setting on the Contact Center Multimedia (CCMM) Administration utility.

Note:

If you migrate from an existing Web Communications chat solution to the EWC chat solution, you must redevelop your custom interfaces to integrate with EWC.

Contact Center database encryption

From Release 7.0 Feature Pack 3, you can encrypt and decrypt the Contact Center database using Security Manager. To encrypt the database, you must create and activate an encryption key and use it to encode the files in the Contact Center Caché database.

Contact Center services secured by default

The Contact Center Release 7.0 base build includes a number of services and connections that you can secure using Transport Layer Security (TLS). By default, Contact Center installs commonly used Web services and CTI connections with security enabled. This feature includes enhancements to the Contact Center Certificate Management tool to make it easier to manage server and root certificates.

On a new Contact Center install, the following connections and services use TLS by default:

- Contact Center Manager Administration (CCMA)
- Contact Center Multimedia (CCMM) Administration
- Agent Desktop
- Multimedia Services
- Orchestration Designer
- Outbound Campaign Management Tool
- Contact Center Web Services
- Communication Control Toolkit (CCT) Web Administration

You can turn off Web services security after installation and initial configuration. If you choose to leave Web Services security enabled, replace the Contact Center default security store with a new security store containing a signed server certificate and root certificate from your Certificate Authority (CA).

Database Integration Wizard configuration moved to Contact Center database

From Release 7.0 Feature Pack 1, Contact Center stores configuration information for the Database Integration Wizard (DIW) in the Contact Center database. The standard Contact Center backup includes this information, so you no longer back up the DIW configuration separately.

When you migrate from an earlier release of Contact Center, you must back up the Database Integration Service configuration from the registry in the normal way. After you restore this configuration to the registry on the new server, Contact Center automatically copies the configuration into the database on the next restart.

Database restore not required for reinstating Mission Critical High Availability

After a managed switchover, administrators do not need to restore the database from the new active server to the standby server to re-instate HA.

A managed switchover is a switchover initiated by the administrator or caused by a Contact Center software service outage.

Data Management - customer privacy

From Release 7.0 Feature Pack 3, you can use the Multimedia Data Management utility to act on privacy requests from contact center customers. For example, if a customer exercises their right to access information or their right to be forgotten, you can use the Multimedia Data Management utility to satisfy these requests.

File extension restrictions for attachments

From Release 7.0 Feature Pack 1, Contact Center administrators can use the Contact Center Multimedia (CCMM) Administration utility to configure the supported list of file extensions that agents can attach to emails. When agents add a file attachment to an email, Agent Desktop displays the configured list of file attachment extensions in the Open dialog box. If the attachment type is not in the configured list, Agent Desktop displays a warning message and does not attach the file to the email.

Increased CCMM customer contact ratio

From Release 7.0 Feature Pack 2, the customer to contact ratio in Contact Center Multimedia (CCMM) has been increased to 1:1000 (or 1 customer record per 1000 contacts).

Instant Messaging feature supports Microsoft Skype for Business 2015

From Release 7.0 Feature Pack 1, the Contact Center Instant Messaging feature integrates with Microsoft Skype for Business 2015. Integration and operation is identical with releases of Microsoft Lync already supported in the Contact Center 7.0 base release.

Interoperation with Avaya Context Store Snap-in using HDX

Avaya Aura® Contact Center (AACC) flow applications can inter-operate with Avaya Context Store Snap-in using HDX commands. Context Store Snap-In Release 3.2 includes a SOAP API and associated Web service that enables AACC flow applications to use Host Application Integration (HAI) calls to access Context Store data.

You create the Web service in the normal way using the Database Integration Wizard (DIW). AACC flow applications can use the Web service Provider ID to send requests and get responses from Context Store.

Modify chat transcripts of Enterprise Web Chat

From Release 7.0 Feature Pack 1, Contact Center administrators can modify chat transcripts of Enterprise Web Chat (EWC) before the transcripts are saved to the Multimedia database.

Creating filters is the responsibility of the customers and a sample filter is provided as part of the EWC SDK. Administrators can configure EWC to use a transcript filter created by the customer. The transcript filter can be used to modify the transcript to mask sensitive data such as account details, credit card numbers, or personal identification numbers. The transcripts are associated with the customer record whose email sent the chat request.

Multimedia account passwords must meet minimum complexity criteria

From Release 7.0 Feature Pack 1, Contact Center requires multimedia accounts to meet the minimum password complexity criteria. If you are an agent or supervisor who handles multimedia contacts, Agent Desktop forces you to change your password if you log on using the default password or your password that does not meet the minimum password complexity criteria.

Passwords must fulfill the following complexity criteria:

- Must be between 8 to 20 characters
- Must contain a number

- Must contain at least one uppercase letter and at least one lowercase letter
- Must not contain spaces
- Must not contain any of these characters: \ & : < > |

Agents can change the multimedia account password using the **Preferences** tab in the User Preferences screen. Administrators also can change multimedia account passwords using the Multimedia Administration utility.

Offline Security Store

From Release 7.0 Feature Pack 2, you can create an offline store using Security Manager. This allows you to minimize downtime if you want to replace your current security store. When your offline store is created, you can swap between the active store and the offline store. You can make the offline store the active store at any point using Security Manager. You must stop Contact Center services before making the offline store active.

Provision of adding a friendly name for a web chat agent

From Release 7.0 Feature Pack 1, Contact Center administrators can add a friendly name or nickname for a web chat agent. If administrators configure the Friendly Name label, the nickname of the web chat agent is displayed in agents' responses to web chat messages. Administrators can also choose that the friendly name is displayed in welcome messages.

Removal of the default Agent Desktop Dashboard password

From Release 7.0 Feature Pack 1, Contact Center has removed the default password that was required to access Agent Desktop Dashboard. You can collect and upload log files or videos to the Contact Center server without entering a password.

REST API Enhancements

From Release 7.0 Feature Pack 3, the Contact Center REST API supports GET, POST, PUT, or DELETE request methods. Using the TFE REST Configurator, you can now add environments which enable the use of environment variables in REST requests.

Contact Center workflows now support the CONVERT and JSON GET ELEMENT command.

REST API integration

From Release 7.0 Feature Pack 2, Contact Center allows you to invoke REST API in a Contact Center workflow. REST (Representational state transfer) provides efficient scalable services for web communications.

A Contact Center workflow can request data using scripting commands, and the workflow uses the TfeRestService to request and retrieve data from the REST API.

Security Manager support for chained certifcates

From Release 7.0 Feature Pack 3, Security Manager supports importing chained certificates.

Server Message Block signing enabled on Windows Server 2012

From Release 7.0 Feature Pack 1, both the Contact Center DVD and the Release Pack installer modify the Windows Server 2012 local group policy to enable Server Message Block (SMB) signing. SMB signing places a digital tag into each server message block, which helps prevent man-in-the-middle attacks on network file sharing.

If you do not want to use SMB signing, you can disable it by modifying the Windows Server 2012 local group policy.

Supervisors can change prompts with new Announcement Recorder

From Release 7.0 Feature Pack 1, Contact Center includes a new Announcement Recorder application. The Announcement Recorder is a Telephony User Interface (TUI) that supervisors and supervisor agents can use to change prompts used in Contact Center flows.

This feature requires that you license and configure Agent Greeting. Supervisors and supervisor agents that want to use the application must be enabled for Agent Greeting.

Whisper Coaching

From Release 7.0 Feature Pack 1, SIP-enabled Contact Centers extend the Supervisor Observe feature to include Whisper Coaching. Using Whisper Coaching, a supervisor can talk to an agent on a skillset call with a customer, without being heard by the customer. In the coaching mode, a supervisor can hear everything that is said on the call. However, the advice that the supervisor provides is audible only to the agent.

Whisper Coaching improves agent training and performance because supervisors can coach the agent by whispering advice to the agent.

Other changes

Other changes in the Release 7.0 base build

See the following sections for information about other changes in the Release 7.0 base build:

- Avaya Media Server changes on page 34

Other changes in Release 7.0 Feature Pack 1

See the following sections for information about other changes in Feature Pack 1:

- Automated backup of new security store on page 34
- Contact Center implements Transport Layer Security version 1.2 by default on page 35
- iceAdmin account privileges reduced on page 36

Automated backup of new security store

From Release 7.0 Feature Pack 1, Contact Center automatically backs up a new security store when you create it. This allows you to recover from situations where the store is damaged or deleted before you make a manual backup of the store.

Avaya Media Server changes

Avaya Media Server is now called Avaya Aura® Media Server. Avaya Aura® Contact Center Release 7.0 supports only Avaya Aura® Media Server Release 7.7.

Avaya Aura® Contact Center Release 7.0 no longer requires or uses the Contact Center Services for Avaya Media Server (CCSA) component. Avaya Aura® Contact Center Release 7.0 integrates directly with Avaya Aura® Media Server Release 7.7 using Media Server Markup Language (MSML) based communication.

Avaya Aura® Contact Center and Avaya Aura® Media Server use MSML to control how Route Point calls are anchored and treated. Avaya Aura® Contact Center also uses MSML to control Route Point call features such as Agent Greeting, Barge-in, Observe, Zip Tone, and Whisper Skillset announcements.

In Contact Center Manager Administration (CCMA) *Media Services and Routes* configuration, Avaya Aura® Media Server Release 7.7 instances now provide a new MSML-based service type named ACC_APP_ID. This new ACC_APP_ID service type replaces the CONF service type provided by Avaya Media Server Release 7.6.

The following features, previously configured in Avaya Media Server Element Manager, are now configured in Contact Center Manager Administration (CCMA).

- Barge-in tone
- Observation tone
- Call Force Answer Zip tone
- Custom Zip tones
- Whisper Skillset announcement

Enable or disable Barge-in and Observation tones in CCMA *Global Settings*.

Upload the tone and announcement .WAV files in CCMA *Prompt Management*.

Configure Call Force Answer Zip Tone and Whisper Skillset in CCMA *Call Presentation Classes — Prompt On Answer*.

Avaya Aura® Media Server supports only the following deployment options:

- Co-resident with Avaya Aura® Contact Center on a Windows Server 2012 R2 server
- Standalone on a Red Hat Enterprise Linux 6.x 64–bit server

Avaya Aura® Media Server is also available as an Open Virtual Appliance (OVA) package. You can use this OVA file to create an Avaya Aura® Media Server virtual appliance on a VMware host.

Virtualized Avaya Aura® Media Server supports High Availability (HA).

Contact Center implements Transport Layer Security version 1.2 by default

From Release 7.0 Feature Pack 1, Contact Center implements Transport Layer Security (TLS) version 1.2 as the default minimum version negotiated for secure communications. This is to avoid security vulnerabilities that exist in TLS 1.0.

Before migrating to Release 7.0 Feature Pack 1, ensure that the browsers you use for CCMA or Element Manager are configured to use TLS 1.2.

For backward compatibility and inter-operation with third-party or custom applications connecting to Contact Center, Administrators can set lower versions of TLS on certain communication channels. When a lower version of TLS is available, Contact Center still negotiates the highest level of TLS that the other application can support.

Before migrating from a previous Release, or before applying Feature Pack 1 to a Release 7.0 solution, check third-party or custom applications that connected securely to Contact Center, to understand whether you need to change the Contact Center TLS versions.

If you apply Feature Pack 1 to an existing Release 7.0 installation, Contact Center does not apply this change, and retains your Release 7.0 TLS configuration.

iceAdmin Windows account privileges reduced

From Release 7.0 Feature Pack 1, Contact Center reduces the Windows privileges of the CCMA Administration account, iceAdmin. This is to improve security by restricting iceAdmin to the minimum Windows privileges required for managing CCMA.

This reduction in privileges changes the way you configure network printers for CCMA reports.

Part 1: Contact Center Manager Server

- Contact Center Manager Server fundamentals on page 38
- Contact Center Manager Server configuration on page 46
- Contact Center Manager Server statistics configuration on page 57
- Database Integration Wizard configuration on page 62
- REST API configuration on page 79

Chapter 3: Contact Center Manager Server fundamentals

This chapter provides an overview of the Contact Center Manager Server (CCMS) tools and utilities.

Host Application Integration service functionality

The Contact Center Manager Server installation automatically installs the Host Application Integration (HAI) service. The HAI service enables CCMS flow applications to integrate with the following types of service provider:

- Contact Center or third-party databases, to run queries and procedures.
- Third-party Web services.
- On AML-based solutions, a TAPI database to run queries and procedures.

The connection to the database requires access permissions. Your Contact Center Manager Server HAI service and the Database Integration Wizard must use the correct context to connect to the database.

HAI service integration with HDX

The HDX service maintains connections between CCMS call processing and registered third-party applications. The HAI service is a registered third-party application.

The following is an example of how a call processing flow application uses HDX to access methods from a registered third-party application such as HAI:

1. When the call processing flow application encounters a Host block (for example SEND INFO or SEND REQUEST/ GET RESPONSE), it packages the parameters into a message.
2. The HDX service receives and queues the message. The registered third-party service provider specified in the host block can then use the HDX interface to retrieve the message.
3. The service provider receives the message, unpacks the data it contains, and runs the specified service.

4. If the specified service is a request, the request runs, and the service provider packages the results into a message and returns them to HDX.
5. When HDX receives the message, it routes the data to the flow application.
6. The flow application receives the message, unpacks the data, and maps the values to the Response Parameters call variables.

Contact Center Manager Server flow applications use provider IDs to identify different HDX applications. The HAI service registers with HDX as a third-party application with a unique provider ID. You configure this provider ID in the Database Integration Wizard. All the third-party database, Web service, and TAPI connections that you define in the Database Integration Wizard use this single provider ID. Avaya recommends that you use a global variable rather than a call variable for the provider ID when creating flow applications in Orchestration Designer. If you need to change the HAI provider ID in the Database Integration Wizard, then you can change the corresponding value in the global variable in Orchestration Designer, and you do not need to recompile all the applications that use the HAI service.

After registering with HDX, the HAI service enables the exchange of data between Contact Center Manager Server flow applications and:

- any Open Database Connectivity (ODBC) 3.51 compliant database
- any Web service for which you have access to the Web Service Description Language (WSDL)

On AML-based systems, you can also use the Database Integration Wizard to configure the HAI service to register with the TAPI server. After you register the service with the TAPI server, flow applications can attach data to a call.

HDX provides a maximum of 10 client application connections. HAI is a HDX client application, and uses one of the 10 available HDX connections. When you configure and activate HAI in the Database Integration Wizard, there are nine HDX client application connections available for use with other third party client applications. The HDX limit for the size of a data parameter is 80 bytes.

Configuring the HAI service in the Database Integration Wizard

You must use the Database Integration Wizard (DIW) to configure the HAI service if you want to use the service from flow application Host blocks. If you plan to use a third party database, in Windows Server 2012 you must configure a Data Source Name (DSN) for that database before you configure HAI. The Contact Center DSNs are available in DIW by default. Use the DIW to configure the HAI provider ID and the following options:

- The TAPI provider. Only AML-based solutions can use this option.
- Connections to Data Source Names (DSNs) for databases that you plan to access from flow applications.
- Connections to Web services that you plan to access from flow applications.
- Statements to run on Contact Center and third-party databases, either as SQL commands or stored procedures.

- Statements to access configured Web service methods.

Interaction with application commands

After you use the Database Integration Wizard to configure the HAI service, you can use flow application Host blocks for HDX to integrate with HAI.

When HAI retrieves a message from HDX, HAI checks the message type:

- SEND REQUEST/GET RESPONSE commands are for database or Web service read access, and, where available, for data retrieval from TAPI.
- The SEND INFO command is for database or Web service write access, and, where available, for attaching TAPI call data.

The first parameter of SEND REQUEST or SEND INFO specifies whether the command is for database or Web service access, or for TAPI access. If the command is for database or Web service access, the first parameter is the unique number of the statement or method to run. If the command is for TAPI access, the first parameter is always %TAPI%.

SEND REQUEST and GET RESPONSE

You implement SEND REQUEST and GET RESPONSE commands in a flow application using a Host block with the **Request/Response** option. The Host block hides the details of the actual HDX command syntax. The SEND REQUEST and GET RESPONSE commands retrieve information from a database, from a Web service, or from TAPI.

The first parameter of the SEND REQUEST command determines whether the target is database access / Web service, or TAPI. If the first parameter is %TAPI%, Contact Center requests information from TAPI. If the first parameter is not %TAPI%, then it must be the number of a statement already configured in Database Integration Wizard to access a database or Web service.

The remaining Request parameters provide information to the unknown parameters of the statement configured in the Database Integration Wizard. The Host block must specify an input variable for each unknown parameter configured in the DIW statement. The type of each input variable must match the data type required by the SQL query or Web service method.

In DIW, you identify each unknown parameter with a question mark (?) in the statement. You can use up to nine parameters.

All HDX request messages have a matching GET RESPONSE message. The first parameter of the GET RESPONSE message specifies the status of the statement execution. The first parameter of the GET RESPONSE is reserved as a string variable to store the status of the SQL procedure. The returned value is one of the following:

- SUCCESS. The statement ran successfully.
- FAILED. The statement failed. Examine the log files to determine the reason for failure (for example, attempting to run an invalid SQL statement results in a FAILED operation).
- NODATA. The statement is of type SELECT; however, no data was returned.

Returned data from the statement execution populates the remaining message parameters. All remaining parameters of the GET RESPONSE message have a default value of NULL, which is represented within the flow application as a blank value for a string, or a zero for an integer.

HAI packages the returned data in a service completion message, and passes it back to HDX.

If the GET RESPONSE command returns data from a CCT/TAPI application, each piece of data must be separated by a RECORD_SEPARATOR, defined as follows:

- `#define RECORD_SEPARATOR 0x1E`

The RECORD_SEPARATOR ensures that each piece of data can be supplied separately in the GET RESPONSE command.

You must check each SQL query configured in the Database Integration Wizard to ensure that it does not use an excessive amount of time to run. By default, the GET RESPONSE command waits 10 seconds for the query to execute before it times out. If the GET RESPONSE command times out, the flow application continues without the response. Depending on the nature of the query, this can disrupt call processing.

If an SQL query runs longer than 10 seconds, you can perform one of the following activities:

- Optimize the SQL query so that it takes less time to execute (for example, rewrite the query or use stored procedures).
- Use the optional **Timer** option in the Host block to increase the timeout value.

SEND INFO

You implement a SEND INFO command in a flow application using a Host block with the **Send Info** option. The host block hides the details of the actual HDX command syntax.

HDX uses the SEND INFO command to write data to a database, send data to a Web service, or attach data to a call by using TAPI. The first parameter of the SEND INFO request identifies whether the target is database access or TAPI. If the first parameter is %TAPI%, the remaining parameters are attached to the call using the IVR/CallData interface provided by TAPI. When attached to the call in TAPI, each data parameter is separated by a RECORD_SEPARATOR.

If the first parameter is not %TAPI%, then it must be the number of a statement already configured in Database Integration Wizard to send information to a database or to a Web service. For example, the numeric identifier can identify a statement, such as an SQL UPDATE, that does not return data to Contact Center. The same principles with regard to parameters described for SEND REQUEST/GET RESPONSE apply to SEND INFO when you use it for database access or for a Web service.

Often, multiple HAI service actions occur sequentially in the flow application for a single contact. When the result of one action depends on a previous action being completed fully, ensure that the first action is fully complete before the next action is executed.

You must change the following registry keys to sequentially run flow application commands:

```
\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nortel\ICCM\HAI\Threads
\WorkerThreads value=1
```

```
\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nortel\ICCM\HAI\Threads
\WorkerThreadsSleep value=60
```

Stored procedures

The HAI service in Contact Center Manager Server supports the use of stored procedures on the Contact Center or third-party database server. Stored procedures are precompiled sets of SQL statements you create in, and the system stores on, the database server.

HAI invokes stored procedures by using conventions appropriate to the database vendor.

To use stored procedures, you must add them as statements in the Database Integration Wizard.

You can create stored procedures on a database server by using the database server software. For instructions to create stored procedures, refer to your database vendor documentation.

Using complex SQL statements in Microsoft SQL Server

Executing an SQL statement when the database is configured to return the number of rows affected by that Transact-SQL statement or stored procedure can return invalid results as the number of rows affected is returned as part of the results. To ensure the SQL statement runs successfully, use the SET NOCOUNT ON setting to prevent the counting of the number of rows to be affected.

Using stored procedures that support SELECT...INTO only

When you use stored procedures that support only the SQL construction of SELECT... INTO, invoke the procedures in the following order:

- SEND INFO, to invoke the stored procedure
- SEND REQUEST and GET RESPONSE, to retrieve the data put into the variables by using the SQL construction of SELECT...INTO

The threading model in HAI can make the system process the SEND INFO and SEND REQUEST commands in the wrong order. If this happens, the script receives invalid data. To guarantee the order of the commands, set the value of the following registry key to 1:

\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nortel\ICCM\HAI\Threads

The default setting has two worker threads, which provides fast performance but does not guarantee order of execution.

If you adjust the worker thread setting, you must also adjust the sleep timer setting. The default value for the sleep timer is 120.

Using stored procedures in Oracle

When a stored procedure must return data to the script, the stored procedure must prepare the data in a form that can be retrieved by HAI. The data must be available to provide information for the parameters of a GET RESPONSE request. Some databases support output parameters where the data is returned in parameters when the procedure is called. This data is not available to HAI and this type of stored procedure is not directly supported by HAI. For example, parameters can be identified as OUT in Oracle. The data passed in the OUT parameter cannot be retrieved by HAI.

Feature report

The feature report provides easy access to the system attributes on the Contact Center Manager Server:

- Customer name
- Company name
- Site name
- Avaya Subnet IP address
- Contact Center Manager Server license type
- Contact Center Manager Server version

Multicast Address and Port Configuration

Use the Multicast Address and Port Configuration utility to change the default data for the optional Real-Time Statistics Multicast (RSM) feature. You can change the following settings:

- the IP multicast address to which each server in Contact Center Manager Server sends real-time statistics
- the ports at which real-time statistics are received
- the multicast Time to Live (TTL) value for RSM
- the default multicast rate for each port at which real-time statistics are received
- the version of the RSM stream to use

Multicast Stream Control

Use this utility to modify settings for applications that require that real-time statistics be turned on manually.

The real-time statistics groups that you need to turn on or off vary depending upon the applications that receive data from the RSM service. Avaya recommends that you review the documentation for each RSM-dependent application in Contact Center Manager Server before you modify the RSM settings.

Network Configuration utility

Use the Network Configuration utility, Nbconfig, to view the local server settings, the address table, and the sites for your Contact Center Manager Servers.

If your contact center is in a networked environment, you can use the Network Configuration utility to add sites to the Network Control Center.

The following access levels are available:

- regular access level—Read the information in the Network Configuration utility.
- administration access level—Change the server settings.

You can view the following information in the **Nbconfig** dialog box:

- Local Machine Settings—The **Local Machine Settings** tab lists the local site name and network card IP addresses.
- Address Table—The **Address Table** tab lists the computer name, IP address, and port information of all servers in the network, including the Network Control Center.
- Site Table—The **Site Table** tab lists information about site names, IP addresses, and flags. When you log on to the Network Control Center in administration mode, use this page to add sites.

Important:

Ensure that the Nbconfig utility is not running while Contact Center services are starting.

Server configuration

Use the Contact Center Manager Server Configuration utility to modify the data completed during the initial installation of the Contact Center Manager Server. You can change the local settings, the licensing, SIP Network settings, SalesForce, the Communication Server 1000 information, Call Pilot settings, Communication Control Toolkit Server, and WS Open Interfaces information.

For information about working with the Configuration utility, see the following sections:

- Changing the local settings configuration on page 47
- Changing the licensed features configuration on page 48
- Changing the Avaya Communication Server 1000 PABX data on page 50

Web services

The Open Queue Open Interface delivers existing Open Queue functions to third-party applications that use a Web service. Third-party applications can add and remove contacts of a specific type in the Avaya Aura® Contact Center.

For more information, see the SDK documentation.

The Open Networking Open Interface enables a third-party application to transfer a call between nodes in a network with any data associated with that call intact. Third-party applications can reserve a Landing Pad on the target node to enable the voice contact to be transferred with data attached. The Web services also provide a function to cancel the reserving of a Landing Pad freeing it for other calls to be transferred across the network.

For more information, see the SDK documentation.

Chapter 4: Contact Center Manager Server configuration

This chapter describes how to change the configuration properties for the Contact Center Manager Server software on your server.

Use the Server Configuration utility to make these changes.

Note:

In a High Availability solution, you must manually make the same changes on the Standby server as you make on the Active server. There are two exceptions to this:

- The Avaya Server Subnet IP Address
- The ELAN Subnet IP Address

Ensure you repeat each procedure in this chapter on the Standby server.

Prerequisites to Contact Center Manager Server configuration

Procedure

Commission Contact Center Manager Server. See *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.

Starting the Network Configuration utility

About this task

Start the Network Configuration utility with regular access level to read the information about the local machine settings, the address tables, and the site table for your contact center.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Network Configuration**.

2. Click each tab to view the content.
3. Click **OK**.

Changing the local settings configuration

Before you begin

- Depending on the changes you make, this procedure can require restarting the server.

About this task

Change the Contact Center Manager Server (CCMS) local configuration settings, after you install the CCMS software, to change the names and IP addresses required for Contact Center to run.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
2. In the **Server Configuration** dialog box, click the **Local Settings** tab.
3. Update the local settings.
4. Click **Apply All**.
5. If the Contact Center Server Configuration application displays a **Restart Required** dialog, click **Yes**.
6. Click **Exit**.

Variable definitions

Name	Description
Company Name	The name of the company that uses the Contact Center Manager Server software.
Customer Name	The designated contact person at the company that uses Contact Center software.
Avaya Server Subnet—IP Address	The IP address of the subnetwork that connects the Contact Center servers (Contact Center Manager Server, Network Control Center, Contact Center Manager Administration, Contact Center Multimedia, and (optionally) Avaya CallPilot®) are connected.
ELAN Subnet—IP Address	The IP address of the embedded local area network, a dedicated Ethernet LAN that connects the Contact Center Manager Server and the PABX.

Table continues…

Name	Description
	You must select the check box for the ELAN Subnet IP Address if you use an ELAN subnet.
Real-Time Statistics Multicast IP Address	The RSM IP address of the server to associate with sending real-time data. The IP address must be 224.0.1.0 to 239.255.255.255. The default is 230.0.0.1.
Site Name	The site name for the Contact Center Manager Server. The site name must not contain spaces or non alphabetical characters except for hyphen (-) and underscore (_). The first character must be a letter. The site name must be unique and can consist of any combination of 6 to 15 characters.

Changing the licensed features configuration

About this task

Change the licensing configuration of the Contact Center Manager Server, after you install the Contact Center Manager Server software, to update the licensing details.

You can use this application to enable or disable the features of Contact Center including open queue and networking.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
2. In the **Server Configuration** dialog box, click the **Licensing** tab.
3. Update the licensing details.
4. Click **Apply All.**
5. If the Contact Center Server Configuration application displays a **Restart Required** dialog, click **Yes**.
6. Click **Exit**.

Variable definitions

Name	Description
Package	The installation package indicates the licenses that you purchased with Contact Center: • Nodal Enterprise: The base package for Contact Center on the current supported switching platforms. • Corporate Enterprise: The networking package.
Features	You must choose the package you purchased. Packaged features include: • Networking—Agents and skillsets are configured on a Network Control Center (NCC) and propagated to network servers. If a server has a local skillset with the same name as a network skillset, the network skillset replaces the local skillset. • Universal Networking—Universal Networking is the networking between switch types: - Network Skill-based Routing between all switch types supported by Contact Center - attached data transport during agent-initiated transfers or conferences under the control of the Communication Control Toolkit • IM—Use the Instant Message (IM) feature to allow agents to communicate with customers over the Internet in real time. • Web Based Statistics: Use Agent Web Statistics on Agent Desktop, so that agents and supervisors can use Agent Desktop to view real-time statistics for call handling, skillset data, and state information on Agent Desktop. • Multiplicity—Use Multiplicity to ensure an agent can handle multiple concurrent contacts. At any one time an agent can be active on a voice and multimedia contact; only one of these can be active, the others automatically are on hold. • Open Queue—Use Contact Center Multimedia to route multimedia contacts to agents by using the existing scripting and skillset routing features available for calls. You must install and license the Open Queue feature for Avaya Agent Desktop

Table continues…

Name	Description
	and configure Open Queue on the Communication Control Toolkit server. • OI Open Queue—The Web services are a series of Open Interfaces provided to third parties to enable application communication based on the SOA architecture. The Web services ensure customers can discover the functions offered by each Web service using the WSDL provided. • OI Universal Networking—Use Network Skill-Based Routing to route voice contacts between networked sites in a mixed PABX environment. • Agent Greeting—Use the Agent Greeting feature to allow agents to pre-record greetings. Contact Center plays the greeting automatically when an agent answers a call. The Agent Greeting feature is supported only in SIP-enabled contact centers. This license also enables the Announcement Recorder application, which supervisors can use to modify announcements from their telephones. • OffSite Agent—Use Offsite Agent to allow a Contact Center to extend to an agent's preferred environment, allowing them to handle skillset calls regardless of location. The Offsite Agent feature is supported only on the Avaya Aura® Unified Communications platform.
Serial Number	In an AML-based Contact Center, this is the serial number for the Avaya Communication Server 1000. You must obtain the serial number from your distributor. This value is not used in SIP-enabled contact centers.

Changing the Avaya Communication Server 1000 switch data

About this task

Change the Avaya Communication Server 1000 switch data after you install Contact Center Manager Server to enable communication with the Avaya Communication Server 1000 switch.

You can also configure an alternate Avaya Communication Server 1000 switch.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.

2. In the **Server Configuration** dialog box, click **Switch CS1000**.
3. Update the Avaya Communication Server 1000 switch data details.
4. Click **Apply All**.
5. If the Contact Center Server Configuration application displays the **Restart Required** dialog, click **Yes**.
6. Click **Exit**.

Variable definitions

Name	Description
Switch Name	The name of the Avaya Communication Server 1000 switch. Valid characters for PABX names are A-Z, a-z, 0-9, underscore (_), and period (.). PABX names must begin with an alphabetical character and cannot contain spaces. The last character must not be an underscore or period. PABX names must not exceed 80 characters in length.
Switch IP	The IP address of the Avaya Communication Server 1000 switch.
Switch Customer Number	The customer number for the switch.
Alternative Switch IP	The IP address of the alternate Avaya Communication Server 1000 switch.
Alternative Switch Customer Number	The customer number on the alternate Avaya Communication Server 1000 switch.
Alternative Switch Serial ID	The serial number of the alternate Avaya Communication Server 1000 switch.

Changing the Voice Services configuration

About this task

Configure the Avaya CallPilot® or Avaya Aura® Experience Portal communication details to provide voice services for Avaya Aura® Contact Center.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
2. In the **Server Configuration** dialog box, click **Switch CS1000**.
3. To select Avaya CallPilot® as the voice services provider, select **Call Pilot**.

4. To select Avaya Aura® Experience Portal as the voice services provider, select **AAEP**.
5. If you selected **Call Pilot**, update the **Voice Services Configuration** details.
6. Click **Apply All**.
7. If the Contact Center Server Configuration application displays the **Restart Required** dialog, click **Yes**.
8. Click **Exit**.

Variable definitions

Name	Description
CallPilot ELAN IP Address	If you are using a standalone Avaya CallPilot®, enter the Avaya CallPilot® server ELAN IP address. If you are using Avaya CallPilot® High Availability (CPHA), enter the Avaya CallPilot® Managed ELAN IP address.
Port	The networking port number for the Avaya CallPilot® server. The default port number is 10008.
CPHA Managed CLAN IP Address	If you are using Avaya CallPilot® High Availability, enter the Avaya CallPilot® Managed CLAN IP address.
CallPilot CLAN IP Address	If you are using a standalone Avaya CallPilot®, enter the Avaya CallPilot® server CLAN IP address.

Changing the SIP Local Subscriber data

About this task

Change the SIP local subscriber data after you install Contact Center Manager Server to enable communication with other SIP elements.

Important:

Changes to the SIP Local Subscriber data sometimes require restarting the Contact Center Manager Server. Changes to the SIP Local Subscriber data can require updates to other Avaya Aura® Contact Center components, such as Communication Control Toolkit and Contact Center Multimedia.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
2. In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.
3. Update the SIP Local Subscriber details.

4. Click **Apply All**.
5. If the Contact Center Server Configuration application displays the **Restart Required** dialog, click **Yes**.
6. Click **Exit**.

Variable definitions

Name	Description
Local SIP Subscriber	Information about the environment of the SIP-enabled contact center and how to identify the server within the network.
• Contact Center Name • Domain Name	The registration user name on the registration proxy. Use a suitable user name following the standards in your system. Associated domain name for the SIP-enabled contact center.
Web Service Ports	The Web Service Ports group box appears only if you select Avaya Aura® Presence Services as the IM Provider. • Server Port default is 9100. • Client Port default is 9120.
SIP Server Type	Type of SIP proxy for the contact center integration. Depending on the switch type you select in the Application Selection window, the system automatically sets the specific SIP Server Type as the default.
SIP Server Version	The version of SIP proxy that you have if your SIP Server Type is Aura 6.x. • Blank (none) • 6.1 • 6.2 or Greater To activate the Third Line Enabled check box, you must select 6.2 or Greater in the SIP Server Version field.
Third Line Enabled	Select to enable Third Line Appearance. The SIP Server Version must be 6.2 or Greater to activate this check box.
MS Locale	Locale (including language and dialects) of the system environment.

Table continues…

Name	Description
Local Listening Ports	The SIP Communication protocol accepted by the system for incoming calls. • TCP/UDP Port default is 5060. • TLS Port default is 5061.

Changing the SIP Network Settings data

About this task

Change the SIP network settings data after you install Contact Center Manager Server to enable communication with other SIP elements.

Important:

Changes to the SIP Local Subscriber data sometimes require restarting the Contact Center Manager Server. Changes to the SIP Local Subscriber data can require updates to other Avaya Aura® Contact Center components, such as Communication Control Toolkit and Contact Center Multimedia.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
2. In the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.
3. Update the **SIP Network Settings** details.
4. Click **Apply All**.
5. If the Contact Center Server Configuration application displays the **Restart Required** dialog, click **Yes**.
6. Click **Exit**.

Variable definitions

Name	Description
Voice Proxy Server	Information about the server that provides support for inbound and outbound calls, such as routing a call to an agent telephone.
• IP Address	If the contact center uses an Avaya Aura® Session Manager, enter the IP address of the primary Session Manager here.
• Port	The server listening port. The default port is 5060.

Table continues…

Name	Description
• Network Transport	The SIP Network Transport communication protocol. If there are Contact Center agents using SIP desk phones, or if your solution uses Avaya Aura® Presence Services 7.1 or later, you must ensure that the SIP Network Transport communication protocol is set to TLS. The default port number for TLS is 5061.
CTI Proxy Server	Information about the server that provides support for SIP Computer Telephony Integration (CTI) so that Agent Desktop can acquire and control agent telephones for TR87.
• IP Address	If the contact center uses an Avaya Aura® Application Enablement Services server, enter the IP address of it here.
• Port	For an Application Enablement Services server the default SIP CTI Proxy Server port is 4723.
• Network Transport	The SIP Network Transport communication protocol. For an Avaya Aura® Application Enablement Services server, the default Network Transport communication protocol is TLS.
Backup Voice Proxy Server	Information about the server that provides backup support for inbound and outbound calls, such as routing a call to an agent telephone. Avaya Aura® Contact Center must have a Standby Server license to support a Backup Voice Proxy Server. The only type of Backup Voice Proxy Server supported by Avaya Aura® Contact Center is an Avaya Aura® Session Manager when it is used with an Avaya Aura® Communication Manager.
• IP Address	If the contact center uses an Avaya Aura® Communication Manager and a backup Avaya Aura® Session Manager, enter the IP address of the backup Session Manager here.
• Port	The server listening port. The default port is 5060.
• Network Transport	The Backup Voice Proxy Server transport protocol.
IM Proxy Server	Information about the server that supports the deployment of Instant Message over SIP.
• IP Address • Port • Network Transport	The IP address of the SIP IM Proxy Server. The default SIP IM Proxy Server port is 5222. The IM SIP Proxy Server transport protocol.

Table continues…

Name	Description
IM Provider	Select your IM Provider. • **Microsoft OCS / Lync**. If you are using Microsoft Lync or Microsoft Skype for Business as your IM provider. • **Aura Presence Services**. If you are using Avaya Aura® Presence Services as your IM provider.
XMPP Domain	If using an Avaya Aura® Presence Services server, enter the domain name of the Extensible Messaging and Presence Protocol (XMPP) server.

Enabling support for three Call Appearance lines

About this task

In a SIP-enabled contact center, enable Avaya Aura® Contact Center support for the third Call Appearance line on Communication Manager stations.

Note:

You must restart Avaya Aura® Contact Center at the end of this procedure.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
2. In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.
3. From the **SIP Server Version** list, select **6.2 or Greater**.
4. Select **Third Line Enabled**.
5. Click **Apply All**.
6. If the Contact Center Server Configuration application displays the **Restart Required** dialog, click **Yes**.
7. Click **Exit**.

Chapter 5: Contact Center Manager Server statistics configuration

This chapter describes how to configure Contact Center Manager Server statistics. You can choose to configure the multicast or unicast method of passing statistics from the Contact Center Manager Server to Contact Center Manager Administration server to manage reports.

Important:

You must not change the date backwards. You can change the date and time forwards.

Prerequisites to Contact Center Manager Server statistics configuration

Procedure

Commission Contact Center Manager Server. See *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.

Configuring the Multicast controller

Before you begin

- Ensure that you know the Administrator password.

About this task

Configure the Multicast controller if you want to change the IP Multicast address that CCMS uses to send Real Time Reporting data to CCMA. Multicast is a network addressing method for delivering information to a group of destinations in a one-to-many distribution.

CCMS supports real time data by both Multicast and Unicast methods. CCMA checks first for a Multicast stream, and if this is available, it uses Multicast. If Multicast is not available, CCMA requests a Unicast stream from CCMS. CCMA uses the Unicast delivery method only when Multicast is not available. Therefore to use Unicast delivery, you do not need any additional Contact Center Manager Server configuration.

Procedure

1. Log on to the server on which you installed Contact Center Manager Server as **Administrator**.
2. On the **Apps** screen, in the **Avaya** section, select **Multicast Stream Control**.
3. In the **RTD Multicast Controller** dialog box, select the **Moving Window** or **Interval-to-date** check boxes for the each Real Time statistics group to enable the setting.
4. In the **Compression** section of the window, select the **RTD Compression** check box.
5. Clear the **RSM Compression** check box.

   Important:

   Contact Center Manager Administration Real Time Displays and POM integration do not support RSM compression. Neither of these features works if Contact Center Manager Server implements RSM compression.
6. In the **Version** section, select the version of RSM you want to use from the drop-down list.

   To use the Time in not ready reason statistic, you must select **R6.4**. However, if your contact center has a third-party client that uses the RSM stream, do not change this value until that client is updated to accept the Release 6.4 version of RSM. The **R6.4** setting applies to Contact Center Release 7.x also.
7. Click **Apply**.
8. Click **OK**.
9. On the **Apps** screen, in the **Avaya** section, select **Multicast Address and Port Configuration**.
10. In the **RTD Multicast Configuration** dialog box, in the **Multicast IP group** box, type the multicast IP address that Contact Center Manager Server uses to transmit real time data.

    This must be the same address as the Contact Center Manager Administration server receiving IP multicast address.
11. In the **Multicast Time To Live (TTL)** box, accept the default setting.

    OR

    Type a new value.
12. For the **Interval-to-date** and **Moving Window IP Port** and **Multicast Rate** boxes, accept the default values.

    Important:

    Do not change the default ports.
13. Click **Apply**.
14. Click **OK**.
15. On the **Apps** screen, in the **Avaya** section, select **System Control and Monitor Utility**.

16. Click the **CCMS** tab.
17. In the **Enter password** box, type the Process Monitor – Common Utilities password.
18. Right-click **SDP_Service**.
19. Click **Restart**.

Changing the IP multicast settings

Before you begin

- Review the documentation for each RSM-dependent application that uses the RSM service in Contact Center Manager Server.

About this task

Change the IP multicast settings to configure the applications that receive data from the RSM service. You can change the IP multicast addresses, the Time To Live value for the data, IP ports, and multicast rates for the IP ports that send the real-time statistics.

Procedure

1. Log on to the Contact Center Manager Server server.
2. On the **Apps** screen, in the **Avaya** section, select **Multicast Address and Port Configuration**.
3. In the **Multicast IP group** box, type the IP multicast address that is designated as the sending address for IP multicasting in the Contact Center Manager Server.
4. In the **IP Port** boxes, type the IP port for each statistics group.
5. Change the **Multicast time to live (TTL)** value to a value that is appropriate for your network.
6. To increase or decrease the default multicast rate, in the **Multicast Rate** boxes, type a new rate in milliseconds for each port.
7. Click **OK**.
8. On the **Apps** screen, in the **Avaya** section, select **System Control and Monitor Utility**.
9. Click the **CCMS** tab.
10. In the **Enter password** box, type the sysadmin password.
11. Right-click **SDP_Service**.
12. Click **Restart**.

Variable definitions

Name	Description
Default value	The values of the Multicast rates provided when you install Contact Center Manager Server.
Registry value	The values of the Multicast rates stored in the registries. You can select this value to cancel changes in the rates boxes.

Procedure job aid

When you change a multicast rate in the Configuration utility, you modify the current transmission rate after you click **Apply**. A delay can occur when the new rate is larger than the existing rate, but the change is immediate from the application perspective.

Configuring the multicast rate equal to 0 (zero) disables the statistic. This is the same as disabling the statistic in the Multicast Stream Control utility by clearing the check box of the matching statistic. The behavior is equivalent because both utilities can read and write to the same portion of the registry.

You can observe the delay when you open the Multicast Stream Control and Multicast Address and Port Configuration utilities at the same time and make the changes. Refresh the settings of each utility using the Registry Value and Get Current States of the Multicast Stream Control and Multicast Address and Port Configuration utilities, respectively.

Disconnecting Terminal Services sessions

Before you begin

- Plan to use unicast transmission for statistics.

About this task

Disconnect the terminal services session to use the unicast transmission of statistics from the Contact Center Manager Server to the Contact Center Manager Administration server for reporting purposes.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. On the **Start** screen, click **Administrative Tools** > **Terminal Services**.
3. In the Terminal Services Manager window, in the right pane, click the **Sessions** tab.
4. In the right pane, right-click the session to disconnect, and select **Disconnect**.

5. Click **OK**.
6. Close the Terminal Services Manager window.

Chapter 6: Database Integration Wizard configuration

Use the Database Integration Wizard (DIW) to configure the HAI service. You can use the HAI service to exchange data between Contact Center Manager Server flow applications and:

- Open Database Connectivity (ODBC)-compliant databases, such as the Contact Center databases, or a CRM database.
- Web services, for example, the Context Store SOAP Web service.
- On AML-based solutions, a TAPI database, for example to add call attached data for back-end IVR.

The following limits apply when configuring the HAI service in DIW:

- DIW supports a maximum of 100 Data Source Names (DSNs).
- Within each database connection, DIW supports a maximum 100 SQL statements.
- The maximum total number of SQL statements DIW supports is 10 000.
- For a stored procedure or SQL statement, DIW supports a maximum of 4 000 characters.

TLS configuration

When you configure web services, there are different levels of TLS that you can configure. You can choose from one of the following options:

- Import a WSDL with a secure URL, along with the location of a file containing an X.509 certificate of a trusted Certificate Authority. This option is limited; for example this does not allow client server authentication of a secure web service.
- Use the Advanced TLS configuration option when configuring a web service in DIW, which allows you to manage and use full TLS configurations.

Prerequisites to Database Integration Wizard configuration

Procedure

- Commission Contact Center Manager Server. See *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.

- If you want to access a third-party database, install and commission the database.
- If you want to access a Web service, get the location of the Web Service Description Language (WSDL) document that describes the Web service.

Configuring a data source name for a third-party database

Before you begin

- For third-party database connections, install and configure the software and drivers to enable connection to the external database. Test the database connectivity and the data access capability using the tools and techniques provided by the third-party database vendor.

About this task

To connect HAI to a third-party database, configure the data source name (DSN) for that database. Use the Windows Server 2012 ODBC Data Source Administrator to configure the DSN.

Procedure

1. Open Windows Explorer.
2. Navigate to the `C:\Windows\SysWOW64` folder, and run ODBC Data Sources (32 bit).

   Important:

   The Database Integration Wizard requires DSNs to be added as 32-bit. Do not use ODBC Data Sources (64 bit).
3. On the ODBC Data Source Administrator window, click the **System DSN** tab.
4. Click **Add**.
5. On the Create New Data Source window, select the appropriate driver.

   If the required driver is not present, exit the ODBC Data Source Administrator and install the driver using the driver setup program.
6. Click **Finish**.
7. On the driver-specific setup box, in the **Data Source Name** box, type a descriptive name for the data source.

   This is the name that you see in the Database Integration Wizard when you select a DSN.
8. In the **Description** box, type a description for the data source.
9. Configure the remaining fields for connection to the database.

   The fields you see here depend on the database driver you selected.
10. Click **OK**.
11. Click **OK** to close the ODBC Data Source Administrator window.

Configuring the HDX provider ID

About this task

Configure the HDX provider ID used to register the HAI service with HDX. This unique provider ID registers all the functions that you configure in the Database Integration Wizard, including Web service methods, database queries and stored procedures, and TAPI functions.

Important:

If the database requires Domain User authentication instead of database integral user accounts, then the user context running the Database Integration Wizard must be compatible with the assigned database permissions. If the user context and permissions are not compatible, you cannot connect to the database.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Integration Wizard**.
2. On the Welcome window, click **Next**.
3. On the Configure HDX and TAPI Server Connections window, in the **HDX Connection** section, in the **Provider ID** box, type the provider ID for the HAI service. A provider ID of 0 is invalid.

   Contact Center Manager Server flow applications use the provider ID to access the functions that you configure in the Database Integration Wizard. Avaya recommends that you do not change this ID after initial configuration. The provider ID must be unique, and if you create other HDX applications for use in Contact Center, these applications must not use the provider ID configured here.
4. Click **Test Connection**.
5. Review the information presented in the **Test Output and Result** box to ensure the test is successful.
6. Click **Next**.

   To configure a database connection now, see Configuring a data source name for a third-party database on page 63.
7. On the Configure Database Connections window, click **Next**.

   To configure a Web service now, see Configuring Web services on page 67.
8. On the Configure Web Services window, click **Next**.
9. On the Construct SQL Statements window, click **Next**.
10. On the Complete window, click **Finish** to accept the changes and close the wizard.

Configuring TAPI server settings

Before you begin

- Ensure a TAPI server is operational on the network.
- Ensure that you know the TAPI server host name or IP address and the port configured in TAPI for the IVR or CallData interface. Consult your TAPI configuration and TAPI documentation for further information.
- Configure the HDX provider ID

About this task

On AML-based solutions, configure TAPI server settings if you want to integrate your CCMS flow applications with the TAPI database, and attach data to calls.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Integration Wizard**.
2. On the Welcome window, click **Next**.
3. On the Configure HDX and TAPI Server Connections window, in the **HDX Connection** section, in the **TAPI Connection** section, select **Configure Tapi connection**.
4. In the **TAPI Server HostName** box, type the host name or the IP address of the TAPI server.
5. In the **IVR Port** box, type the port number of the IVR/CallData interface.

   This port is usually configured for port 5000. However, TAPI configuration allows a custom port. Consult your TAPI configuration to determine the actual port.

   Important:

   The port you select must be outside the 5000 to 5010 range.
6. Click **Test Connection**.
7. Review the information in the **Test Output and Result** box to ensure the test is successful.

   Important:

   If a failed condition is reported in the **Test Output and Result** box, check that the TAPI Server HostName and IVR port match the target TAPI server. If required, correct the configuration information and test it again. If the failure persists, ensure that the TAPI Server HostName is accessible and that the IVR port is correctly registered on the TAPI server.
8. Click **Next**.
9. On the Configure Database Connections window, click **Next**.
10. On the Configure Web Services window, click **Next**.
11. On the Construct SQL Statements window, click **Next**.
12. On the Complete window, click **Finish** to accept the changes and close the wizard.

Procedure job aid

If a failed condition is reported in the **Test Output and Result** box, check that the TAPI Server HostName and IVR port match the target TAPI server. If required, correct the configuration information and test it again. If the failure persists, ensure that the TAPI Server HostName is accessible and that the IVR port is correctly registered on the TAPI server.

The following table describes common error messages you can receive when you configure HDX and TAPI server settings.

Error message	Description
Already Connected	Contact Center Manager Server Database Integration is already connected to HDX.
Authorization Failed	The user details supplied are incorrect. This message indicates that the version of Contact Center Manager Server Database Integration is different from the HDX version. Contact Avaya Support.
Error	The connection cannot be performed. Contact Avaya Customer Support.
Incompatible Version	The version information supplied is incorrect. This message indicates that the version of Contact Center Manager Server Database Integration is different than the version of HDX. Contact Avaya Support.
Invalid Object	The HDX server object cannot be found, which indicates the HDX service is not running.
The Host could not be found	A server with the specified host name or IP address cannot be found on the network.
Invalid Provider ID	The provider ID entered is invalid. The valid range for a provider ID is 0 to 1999999999.
Too Many Connections	All HDX connections are used. Deregister another HDX provider to free a connection.

Configuring database connections

Before you begin

- Configure the HDX provider ID.
- If you are configuring a third-party database, configure a data source name for the database. See Configuring a data source name for a third-party database on page 63.
- Ensure that you have the correct access permissions to the database, and know the database user name and password that HAI can use to log on to the database.
- If you are already on the Configure Database Connections window, skip to step 4 on page 67.

About this task

Configure a database connection so that HAI can connect to a Contact Center database, or to a third-party database using a DSN that you configured. Specify the user name and password that HAI can use to run SQL commands or stored procedures on the database.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Integration Wizard**.
2. On the Welcome window, click **Next**.
3. On the Configure HDX and TAPI Server Connections window, click **Next**.
4. On the Configure Database Connections window, from the **System DSNs Configured** tree, select the DSN to which you want HAI to connect.

   If you are configuring a connection to a third-party database, this is the DSN you already configured.
5. In the **Username** box, type the user name for the database referenced by this DSN.
6. In the **Password** box, type the password for the database user.
7. Click **Test Connection**.
8. Review the information presented in the **Test Output and Result** box to ensure the test is successful.

   Important:

   If the **Test Output and Result** box shows a failed condition, check the data and correct it as required.
9. Click **Next**.

   To configure SQL statements or stored procedures now, see Creating statements to access a database using SQL or stored procedures on page 70.
10. On the Configure Web Services window, click **Next**.
11. On the Configure SQL Statements window, click **Next**.
12. On the Complete window, click **Finish** to accept the changes and close the wizard.

Configuring Web services

Before you begin

- Configure the HDX provider ID
- Ensure that you have access to the Web Service Description Language (WSDL) document that describes the Web service. Using the Uniform Resource Locator (URL) to the WSDL document, the Database Integration Wizard can generate a corresponding set of statements that use the Web service methods.

- If you are already on the Configure Web Services window, skip to step 5 on page 68.

About this task

If you want to integrate a Web service into Contact Center flow applications, configure the Web service in DIW.

Important:

You cannot use Web service methods that accept a variable number of inputs. This includes methods that take an array or list of variables as a parameter, because HDX can accept only a fixed number of simple data types.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Integration Wizard**.
2. On the Welcome window, click **Next**.
3. On the Configure HDX and TAPI Server Connections window, click **Next**.
4. On the Configure Database Connections window, click **Next**.
5. On the Configure Web Services window, in the **WSDL URL** box, type the address of the WSDL document that describes the Web service.

   The address consists of the URL, the file path, and the WSDL name, and it must end with "?wsdl". For example:

   ```
   http://www.mywebserviceserver.com/filepath/mywsdl?wsdl
   ```

   Important:

   If the Web service uses TLS security, you must use https as the URL prefix.
6. In the **Package Name** box, type a descriptive name for the Web service package.
7. If you want to use the Advanced TLS configuration option, skip to step 9.
8. If the Web service uses TLS security and does not require advanced TLS configuration, in the **X.509 Certificate (Secure Web Services)** box, type the location of the X.509 certificate. You must type the full file path of the file containing the X.509 certificate of a trusted Certificate Authority. Certificates must be in PEM format.

   OR

   Click **Browse** to navigate to the X.509 certificate.

   Skip to step 30.
9. If the secure Web service uses advanced TLS security configuration, click the **Advanced** check box.
10. Click **SSL/TLS Config**.
11. On the **SSL/TLS Configuration** window, click **Add**.

Note:

If you have a previously added configuration that you want to use, select the configuration from the list and click **OK**.

12. On the **Cache SSL/TLS Configuration** window, in the **Configuration Name** box, type a name for the configuration.
13. In the **Description** box, type a description for the configuration if required.
14. Select the **Enabled** check box.
15. For **Type**, depending on the type of authentication required, select either the **Client** or **Server** button.
16. If you require **Server certificate verification**, select the **Required** button.
17. If you enabled server certificate verification, click **Browse** to navigate to the location of the file containing the trusted CA certificates.
18. Navigate to the file location, select the file and click **Open**.
19. If you selected **Client** as the authentication type, you must complete the **This clients credentials** section. If you selected **Server** as the authentication type, skip to step 26.
20. Under **File containing this clients certificate**, click **Browse** to navigate to the location of the file containing the X.509 certificate for this configuration.
21. Navigate to the file location, select the file and click **Open**.
22. Under **File containing associated private key**, click **Browse** to navigate to the location of the private key file for this configuration.
23. Select **RSA** or **DSA** as the **Private key type**.
24. If required, in the **Private key password** box, type the password used to decrypt the private key.
25. Confirm the password in the **Private key password (confirm)** box.
26. Under **Cryptographic settings**, select the versions of SSL and TLS required for this configuration.
27. In the Enabled ciphersuites box, type the list of enabled ciphersuites.

    Note:

    The default value is `ALL:!aNULL:!eNULL:!EXP:!SSLv2`, which disables anonymous, unencrypted, and SSLv2 ciphersuites.

28. Review your configuration, and click **Add**.

    The configuration is added to the list on the **SSL/TLS Configuration** window.

29. On the **SSL/TLS Configuration** window, select the configuration from the list and click **OK**.
30. Click **Import WSDL**.

The import process can take some time, depending on the size of the WSDL document being processed. After you import the WSDL, the **Package Summary and Result** box shows a summary of the imported methods. If the import is not successful, the reason for the failure appears in the box.

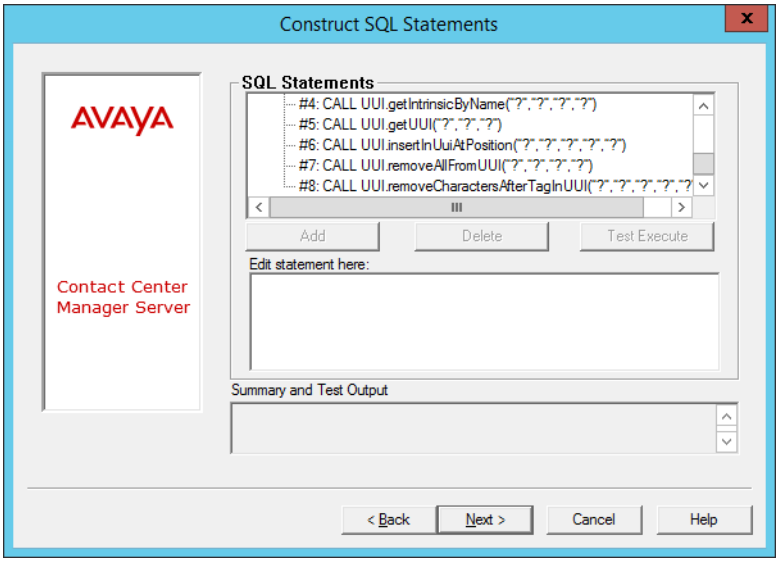
31. Click **Next**.

    Important:

    To immediately test Web service method statements, see Testing statements that use Web service methods on page 72.

32. On the Construct SQL Statements window, scroll down and select Web Services.
33. For the Web service you want to use, note the function number.

    For example, in the following window, we want the service UUI.getUUI. The function is number 5, which you use for the call of the Web service from the CCMS application.



34. Click **Next**.
35. On the Complete window, click **Finish**.

Creating statements to access a database using SQL or stored procedures

Before you begin

- Ensure that you have the correct access permissions for the database.
- If you are already on the Construct SQL Statements window, skip to step 6 on page 71.

About this task

Construct and test a new statement to access a database using SQL, or using an existing stored procedure in the database. You can then use this statement in a flow application to read data from, or write data to, the database.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Integration Wizard**.
2. On the Welcome window, click **Next**.
3. On the Configure HDX and TAPI Server Connections window, click **Next**.
4. On the Configure Database Connections window, click **Next**.
5. On the Configure Web Services window, click **Next**.
6. On the Construct SQL Statements window, select the DSN for the database on which you want to run this statement.
7. To create an SQL statement:
    a. In the **Edit statement here** box, type the SQL statement.

       The statement must include valid sample data for the variable parameters.
    b. Click **Test Execute**.
    c. In the **UserName** box, type the database user name for the selected DSN.
    d. In the **Password** box, type the password for the database user.
    e. Check the **Summary and Test Output** box to see that the test succeeded.
    f. Replace each item of sample data in the statement with a question mark (?).

       Each question mark represents a variable that the flow application passes to the statement.
    g. Click **Add** to add the statement to the DSN.

       Contact Center adds the statement to the SQL Statements list, and automatically assigns a statement number to this statement. You use this statement number to call this SQL statement from a Host block in a Contact Center flow application.
8. To create a stored procedure statement:
    a. In the **Edit statement here** box, type the database stored procedure, followed by valid sample data for the stored procedure parameters.
    b. Click **Test Execute**.
    c. In the **UserName** box, type the database user name for the selected DSN.
    d. In the **Password** box, type the password for the database user.
    e. Check the **Summary and Test Output** box to see that the test succeeded.
    f. Replace each item of sample data in the stored procedure with a question mark (?).

Each question mark represents a variable that the flow application passes to the stored procedure.

g. Click **Add** to add the statement to the DSN.

Contact Center adds the statement to the SQL Statements list, and automatically assigns a statement number to this statement. You use this statement number to call this stored procedure from a Host block in a Contact Center flow application.

9. Click **Next**.
10. Click **Finish** to accept the changes and close the wizard.

Procedure job aid

The results of the execution appear in the **Test Output and Result** box. If the result is not successful, check the statement for errors, correct it as required, and then test it again.

Testing statements that use Web service methods

Before you begin

- Configure the Web service in DIW.
- If you are already on the Construct SQL Statements window, skip to step 6 on page 71.

About this task

Test a Web service method so that you can use it in a flow application. When you configure a Web service, Contact Center automatically assigns statement numbers to all the Web service methods and adds them to the list of SQL statements in DIW.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Integration Wizard**.
2. On the Welcome window, click **Next**.
3. On the Configure HDX and TAPI Server Connections window, click **Next**.
4. On the Configure Database Connections window, click **Next**.
5. On the Configure Web Services window, click **Next**.
6. On the Construct SQL Statements window, in the **SQL Statements** list, expand Web Services.

   The list shows all the methods for imported Web services in the following format:`#<statement number> CALL <WebServicePackageName>.<WebServiceMethod> (<unknownParameters>)`
7. Select the Web service method you want to test.

8. In the **Edit statement here** box, edit the Web service method with valid sample data for the Web service parameters.
9. Click **Test Execute**.
10. Check the **Summary and Test Output** box to see that the test succeeded.
11. Replace each item of sample data in the method with a question mark (?).
12. Click **Update**.

    You can use the statement number to call this Web service method from a Host block in a Contact Center flow application.
13. Click **Next**.
14. Click **Finish** to accept the changes and close the wizard.

Updating an SQL or stored procedure statement

About this task

Update an SQL or stored procedure statement to change the way the statement accesses the database. For example, update the statement if a flow application using the statement needs to get different data from the database, or if you updated the stored procedure that this statement uses.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Integration Wizard**.
2. On the Welcome window, click **Next**.
3. On the Configure HDX and TAPI Server Connections window, click **Next**.
4. On the Configure Database Connections window, click **Next**.
5. On the Configure Web Services window, click **Next**.
6. On the Construct SQL Statements window, on the system tree, select the statement.

   The **Edit statement here** box displays the SQL content or stored procedure for this statement.
7. Edit the statement, replacing the variable parameter question marks with valid sample data.
8. Click **Test Execute** to test the statement.
9. If the test succeeds, replace the variable parameters of the statement with question marks (?), and click **Update**.
10. Click **Next**.
11. On the Complete window, click **Finish** to accept the changes and close the wizard.

Updating a Web service

Before you begin

- Review your flow applications to understand where they have Host blocks that use Web service methods. These blocks can require an update after you update the Web service.
- Note the statement numbers of the existing Web service methods.

About this task

Update a Web service in DIW if the Web service changes.

To update a Web service, you must remove the existing Web service definition, and then re-import the Web service using the updated WSDL document. This process can affect the statement numbers of the Web service methods, because Contact Center assigns statement numbers automatically. It is likely that the statement numbers of the methods will change if:

- The updated Web service includes new methods.
- The statement sequencing changed since you originally imported the Web service, for example due to deleting or adding SQL statements in DIW.

For this reason, Avaya recommends that you always use variables for the statement numbers in your flow applications.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Integration Wizard**.
2. On the Welcome window, click **Next**.
3. On the Configure HDX and TAPI Server Connections window, click **Next**.
4. On the Configure Database Connections window, click **Next**.
5. On the Configure Web Services window, in the **Web Service Packages** section, select the package to remove.
6. Click **Delete Package**.

   A message box appears asking you to confirm the removal of the Web service package.
7. Click **Yes**.
8. In the **WSDL URL** box, type the address of the WSDL document that describes the updated Web service.

   The address consists of the URL, the file path, and the WSDL name, and it must end with “?wsdl”. For example:

   ```
   http://www.mywebserviceserver.com/filepath/mywsdl?wsdl
   ```
9. In the **Package Name** box, type a descriptive name for the Web service.
10. If you want to use the Advanced TLS configuration option, skip to step 12.
11. If the Web service uses TLS security and does not require advanced TLS configuration, in the **X.509 Certificate (Secure Web Services)** box, type the location of the X.509

certificate. You must type the full file path of the file containing the X.509 certificate of a trusted Certificate Authority. Certificates must be in PEM format.

OR

Click **Browse** to navigate to the X.509 certificate.

Skip to step 15.

12. If the secure Web service uses advanced TLS security configuration, click the **Advanced** check box.
13. Click **SSL/TLS Config**.
14. On the **SSL/TLS Configuration** window, select the configuration from the list and click **OK**.

    Note:

    If you want to edit a previously added configuration, select the configuration from the list and click **Edit**. Edit the configuration settings as required. For more information about the configuration settings, see Configuring Web services on page 67.

15. Click **Import WSDL**.

    The import process can take some time, depending on the size of the WSDL document being processed. After you import the WSDL, the **Package Summary and Result** box shows a summary of the imported methods. If the import is not successful, the reason for the failure appears in the box.

16. Click **Next**.
17. On the Construct SQL Statements window, in the **SQL Statements** list, expand Web Services.
18. Check the statement numbers for the methods of the Web service you updated. If the numbers have changed, you must edit the flow applications that use the methods from this Web service.
19. Test each Web service method that the flow applications use.
20. Close the Database Integration Wizard.

Next steps

If the statement numbers of your Web service methods have changed, update your flow application Host blocks with the new statement numbers. Avaya recommends that you always use variables for the statement numbers in your flow applications.

Deleting an SQL statement or stored procedure

About this task

Delete an SQL statement or stored procedure that you no longer use.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Integration Wizard**.
2. On the Welcome window, click **Next**.
3. On the Configure HDX and TAPI Server Connections window, click **Next**.
4. On the Configure Database Connections window, click **Next**.
5. On the Configure Web Services window, click **Next**.
6. On the Construct SQL Statements window, in the **SQL statements** list, select the SQL statement or stored procedure to delete.
7. Click **Delete**.
8. Click **Next**.
9. On the Complete window, click **Finish** to accept the changes and close the wizard.

Removing a Web service

About this task

Remove a Web service package that you no longer require. Ensure that Host blocks in your flow applications do not use any statement number that references a method of this Web service.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Database Integration Wizard**.
2. On the Welcome window, click **Next**.
3. On the Configure HDX and TAPI Server Connections window, click **Next**.
4. On the Configure Database Connections window, click **Next**.
5. On the Configure Web Services window, in the **Web Service Packages** section, select the Web service to remove.
6. Click **Delete Package**.

   A message box appears asking you to confirm the removal of the Web service package.
7. Click **Yes**.
8. Close the Database Integration Wizard.

Configuring the Contact Center Manager Server flow application

Before you begin

- Know the HDX provider ID for the HAI service.
- Create and test a statement in Database Integration Wizard to use an SQL statement, stored procedure, or Web service method.

About this task

The following procedure outlines the high-level steps you take to configure a Contact Center Manager Server flow application to use an SQL statement, stored procedure, or Web service method that you configured in DIW. For detailed information on creating and editing flow applications, see *Using Contact Center Orchestration Designer*.

When using Host blocks to integrate HAI statements, ensure that you:

- Use a global variable for the HDX provider ID that identifies the HAI service.
- Use the return values from the database operation only if the operation was successful.
- Assign values to HDX variables before you use them in a Host block.

Procedure

1. Log on to the Orchestration Designer client.
2. Create a global variable for the HDX provider ID for the HAI service, and give it a value matching the provider ID configured in the Configure HDX and TAPI Server Connections window in the Database Integration Wizard.
3. Create a new flow application, or edit an existing application in which you want to use the DIW statement.
4. Create variables for the DIW statement number, the input parameters, and, if required, the values returned by running the statement.
5. Edit the variable for the DIW statement with the statement number from the Construct SQL Statements window in the Database Integration Wizard.
6. Add a Host block to the flow application.
7. In the Host tab, click **Browse** and select the global variable that contains the HDX provider ID for HAI.
8. If the statement you want to integrate is to request data from a database or Web service:
    a. In the **Host** tab, select **Request/Response**.
    b. In the **Request Parameters** box, use the **Add** button to add the variables for the statement and the input parameters. The variables must be in the correct order as required by the DIW statement.
    c. In the **response parameters** box, use the **Add** button to add the variables for receiving the output values from the DIW statement.

9. If the statement you want to integrate is to send data to a database or Web service:
    a. In the **Host** tab, select **Send Info**.
    b. In the **Request Parameters** box, use the **Add** button to add the variables for the statement and the input parameters. The variables must be in the correct order as required by the DIW statement.
10. Save the HDX block.
11. Complete and activate the flow application.
12. Test the flow application and ensure that it is correctly retrieving data from, or writing data to, the database or Web service.

Chapter 7: REST API configuration

Contact Center allows you to invoke REST API in a Contact Center workflow. REST (Representational state transfer) provides efficient scalable services for web communications.

A Contact Center workflow can request data using scripting commands, and the workflow uses the TfeRestService to request and retrieve data from the REST API.

The Contact Center workflows pass JSON (JavaScript Object Notation) data to the TfeRestService, which identifies the REST API to invoke and populates the REST API parameters. The data returned from the API is reconfigured into a JSON object and then passed back to the workflow. Contact Center supports generic REST API exposed as a URL end-point and query string parameters.

For more information about creating and configuring Contact Center workflows for REST API integration, see *Using Contact Center Orchestration Designer*.

TFE REST Configurator

Contact Center provides an application to configure and test REST API calls. The TFE REST Configurator allows you to configure your REST API end-point and parameters, and to test your configuration. If you receive a successful response after you send the test request, you can then save your configuration to the database. You can use the application to create GET, POST, PUT, or DELETE requests.

You can also add environments using the TFE REST Configurator. Environments enable the use of environment variables. An environment variable is shared across all requests associated with the environment. For example, a service defines a security access token that must be included in the header of all requests for that service. Contact Center provides a default environment named ‘No environment’. You cannot delete this environment. When you create a new request it is automatically associated with the default environment, unless you select an alternative environment that you previously created. The TfeRestService replaces any environment variables in the request with the variable value that you set when creating the environment.

REST API security

Using the TFE REST Configurator, you can configure the following authorization protocols:

- No Auth
- Basic Auth
- OAuth 2.0

Adding a new environment

About this task

Add environments using the TFE REST Configurator. Environments enable the use of environment variables.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **REST Configurator**.
2. In the TFE REST Configurator application, click the Environment settings icon.
3. On the **Environment** window, click the **New environment** icon.
4. In the **Key** and **Value** boxes, type the key and value of the environment variable.
5. Click **Add**.

Creating and testing REST requests

Before you begin

- Ensure that you have all the required REST API end-point and security details, if required.
- Add an environment if required.

About this task

Use the TFE REST Configurator to configure your REST API end-point and parameters, and to test and save your configuration. The TFE REST Configurator supports GET, POST, PUT, or DELETE request methods.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **REST Configurator**.
2. In the TFE REST Configurator application, click the new request icon.
3. From the environment drop-down list, select an environment if required.

   Note:

   The default environment is automatically selected.
4. If security details are required to test the REST API end-point, click the **Authorisation** tab. If security is not required, skip to step 7.
5. Select **Basic Auth** or **OAuth 2.0**.
6. If you select **Basic Auth**:
   a. In the **Username** box, type the user name for the REST API end-point.
   b. In the **Password** box, type the password.

7. If you select **OAuth 2.0**:
    a. To create a new access token, click **New token**. If an access token already exists, skip to step 6h.
    b. On the **Access Token** window, In the **Token Name** box, type a name for the token.
    c. In the **Access Token URL** box, type the URL to access the security token for your end-point.
    d. In the **Client ID** box, type the client ID that identifies the end-point.
    e. In the **Client Secret** box, type the OAuth 2.0 client secret generated for the end-point.
    f. From the **Client Authentication** list, select the authentication method as required for your end-point.
    g. Click **Request**.
    h. From the **Available tokens** list, select the previously created access token.
8. From the request method drop-down list, select the request method for the new request. Select GET, POST, PUT, or DELETE.
9. In the **Please enter request** box, type the request URL.
10. Click the **Parameters** tab to add parameters to the request, if required.
11. In the **Key** and **Value** boxes, type the key value pair to test. You can add multiple key value pairs.
12. Click the **Headers** tab to add header data to the request, if required.
13. In the **Key** and **Value** boxes, type the key value pair of header data to test. You can add multiple key value pairs. The key-value pairs are JSON encoded.
14. Click the **Body** tab to add body data to the request, if required.
15. In the **Key** and **Value** boxes, type the key value pair of body data to test. You can add multiple key value pairs. The key-value pairs are JSON encoded.
16. Click **Execute**.

    The result of the request appears in the **Response** panel.
17. If the request was successful, click the Save icon to add the REST request to the database.
18. On the **Warning** box, click **Continue**.
19. On the **Success** box, click **OK**.

    The REST request appears in the **REST Services** list.

    Important:

    Note the ID of your saved REST requests. The ID is required when you configure your scripts for REST API integration.

Updating a REST request

About this task

Use the TFE REST Configurator to update your saved REST requests.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **REST Configurator**.
2. From the **REST Services** list, select the request to update.
3. Modify the request.
4. Click **Execute** to test the updated request.

   The result of the request appears in the **Response** panel.
5. If the request was successful, click the Update icon to add the REST request to the database.
6. On the **Warning** box, click **Continue**.
7. On the **Success** box, click **OK**.

   The updated REST request appears in the **REST Services** list.

Deleting a REST request

About this task

Use the TFE REST Configurator to delete your saved REST requests from the database.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **REST Configurator**.
2. From the **REST Services** list, select the request to delete.
3. Click the Delete icon.
4. On the **Warning** box, click **Continue**.
5. On the **Success** box, click **OK**.

   The REST request is removed from the **REST Services** list.

Updating an environment

About this task

Update an environment using the TFE REST Configurator.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **REST Configurator**.
2. In the TFE REST Configurator application, click the Environment settings icon.
3. On the **Environment** window, select the environment to edit and click the **Edit environment** icon.
4. In the **Key** and **Value** boxes, edit the values as required.
5. Click **Update**.

Deleting an environment

About this task

Delete an environment using the TFE REST Configurator.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **REST Configurator**.
2. In the TFE REST Configurator application, click the Environment settings icon.
3. On the **Environment** window, select the environment to delete and click the **Delete environment** icon.
4. On the **Warning** box, click **Continue**.

   The environment is deleted.

Part 2: Contact Center License Manager

Licensing administration on page 85

Chapter 8: Licensing administration

The Contact Center License Manager (LM) controls the licensing for the Avaya Aura® Contact Center. The Contact Center License Manager provides central control and administration of application licensing for all of the elements of Contact Center.

There are two modes of Contact Center License Manager deployment. Nodal Licensing mode is used for a single contact center installation. Corporate Licensing mode is used for a network of contact center installations. Corporate licensing supports a secondary Contact Center License Manager, which takes over the licensing if the primary Contact Center License Manager fails.

If CCMS, CCT, CCMM, or CCMA are not able to communicate with the Contact Center License Manager they continue to function for a period of time, called a grace period. If the grace period expires CCMS, CCT, and CCMM shut down and are locked. You cannot restart them without resetting the grace period.

Contact Center License Manager provides central control and administration of licensing for Avaya Aura® Contact Center. Contact Center License Manager supports the following licensing mechanisms:

- **WebLM license file**: Contact Center License Manager can use a local WebLM license file to control Avaya Aura® Contact Center licensed features.
- **Avaya WebLM server**: Contact Center License Manager can obtain licenses from a remote Avaya WebLM server, and then use these licenses to control Avaya Aura® Contact Center licensed features.
- **PLIC license file**: Contact Center License Manager can use a PLIC license file to control Avaya Aura® Contact Center licensed features.

This chapter describes how to configure the Contact Center License Manager for your contact center.

Resetting the grace period

Before you begin

- For Contact Center Manager Server, you must apply separate unlock codes for the CCMS Control Service and the ASM Service. Repeat step 1 on page 86 to step 6 on page 86.
- Obtain a Grace Period Unlock Code from Product Support.

About this task

If the Contact Center Manager Server is not able to communicate with the Contact Center License Manager, normal operation of the Contact Center Manager Server continues for a period of time called a grace period.

If the grace period expires, Contact Center Manager Server shuts down and is locked. You cannot restart Contact Center Manager Server without resetting the grace period.

When a communication error occurs, an event is fired to the Server Utility. The Server Utility records the details, the time elapsed in the Grace Period and a Grace Period Lock Code. These details must be sent to Product Support to obtain a Grace Period Unlock Code. Use this Grace Period Unlock Code to unlock the server and continue working.

Procedure

1. Log on to the server where the Contact Center License Manager software is installed.
2. From the Event Viewer, make a copy of the lock code and send this code to Product Support.
3. On the **Apps** screen, in the **Avaya** section, select **License Grace Period Reset**.
4. Enter the unlock code you received from Product Support.
5. Click **Apply**.
6. Click **Exit**.
7. Restart the Contact Center Manager Server application.

Updating the license file

About this task

Update the license file to upgrade or expand Contact Center Manager Server. You can also change the license file type from PLIC (.lic) and WebLM (.xml) using the License Manager Configuration Tool.

If you are using a remote Avaya WebLM server, see the Avaya WebLM documentation for instructions on applying your updated license file on the Avaya WebLM server.

Procedure

1. Log on to the server where the Contact Center License Manager software is installed.
2. On the **Apps** screen, in the **Avaya** section, select **License Manager Configuration**.
3. Select the **Configuration** tab.
4. If you are changing the license type, in the **License Type** section, select the new license type.
5. Click **Browse**.
6. Navigate the file system and locate the new license file.

7. Click **Open**.
8. On the License Manager Configuration Tool window, Click **Apply**.
9. On the pop-up dialog, click **Yes** to restart Contact Center License Manager.
10. Click **Close** to close the window.

Changing from Nodal to Corporate licensing

Before you begin

- Install Contact Center License Manager on a Contact Center Manager Server or Network Control Center server.
- Use default ports 3998 to 4007 to pass through any firewall between nodes and the Corporate Contact Center License Manager site.
- If your Contact Center License Manager is installed on the same server as Contact Center Manager Server, shut down Contact Center Manager Server.
- Ensure that the primary Contact Center License Manager and secondary Contact Center License Manager can resolve the hostname of each other.
- Plan to restart the server at the end of this procedure.

About this task

Use Corporate Licensing to distribute licenses to multiple servers from a single license pool. You can configure one active Contact Center License Manager and one standby Contact Center License Manager in the Contact Center server network.

Procedure

1. Log on to the server where the Contact Center License Manager software is installed.
2. On the **Apps** screen, in the **Avaya** section, select **License Manager Configuration**.
3. On the License Manager Configuration Tool window, click **Browse**.
4. Navigate the file system and locate the new license file.
5. Click **Open**.
6. On the License Manager Configuration Tool window, click **Apply**.
7. Click **Yes** to restart the Contact Center License Manager Server service.
8. Click **Close** to close the window.
9. Click **Exit**.
10. If you have a Secondary Contact Center License Manager, perform the following steps. Otherwise, proceed to step 20.
11. Copy the new Corporate License file to the appropriate directory on the Contact Center Manager Server serving as the host for the secondary Contact Center License Manager.

12. Shut down the Contact Center Manager Server services on the secondary Contact Center License Manager server. If you do not, the Contact Center Manager Server services shut down due to a refresh error.
13. On the **Apps** screen, in the **Avaya** section, select **License Manager Configuration**.
14. On the License Manager Configuration Tool window, click **Browse**.
15. Navigate the file system and locate the new license file.
16. Click **Open**.
17. On the License Manager Configuration Tool window, click **Apply**.
18. Click **Yes** to restart the Contact Center License Manager Server service.
19. Click **Close** to close the window.
20. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
21. If an information box appears, click **Continue**.
22. Click **Licensing**.
23. Under **License Manager Package**, change the package to the corporate version.
24. Under **License Server IP Address**, in the **License Server IP** field, enter the IP address of the Contact Center License Manager server.
25. Click **Apply All**.
26. Click **Yes** to restart the server.

Changing the licensing information on Contact Center Manager Server

Before you begin

- Shut down the Contact Center Manager Server services on the appropriate server.
- Plan to restart the server at the end of this procedure.

About this task

Change the license manager package information on a Contact Center Manager Server if you purchased additional options listed in the Contact Center Manager Server configuration.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **System Control and Monitor Utility**.
2. Click the **LM** tab.
3. Click **Shut down License Manager**, and wait for the CC_LM service to stop.
4. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.

5. Click **Licensing**.
6. Under **License Manager Package**, change the **Package** and **Features** information to reflect your new licensed options.
7. Under **License Server IP Address**, in the **License Server IP** field, enter the IP address of the Contact Center License Manager server.

   If your contact center uses Nodal licensing, CCMS automatically completes this field.
8. Click **Apply All**.
9. Click **Yes** to restart the server.

Refreshing your server

Before you begin

- Log on as the Webadmin user to refresh the servers.

About this task

Refresh your server if a new license file is configured and accepted by Contact Center Manager Server, or you connect to a different Contact Center License Manager server (that is, a new or standby Contact Center License Manager server), or you have enabled Open Queue.

Procedure

1. Log on to Contact Center Manager Administration.

   Contact Center Manager Administration (CCMA) displays the date and time of your last login and also the number of failed login attempts before a successful login.
2. On the launchpad, click **Configuration**.
3. On the **Server** menu, click **Refresh All Servers**.
4. Click **Yes**.

Configuring remote Avaya WebLM server details

About this task

Configure Contact Center License Manager to use a remote Avaya WebLM server. Contact Center License Manager can obtain licenses from a remote Avaya WebLM server, and then use these licenses to control Avaya Aura® Contact Center licensed features.

Refer to the Avaya WebLM documentation for instructions on applying your updated license file on the remote Avaya WebLM server.

Procedure

1. Log on to the server where the Contact Center License Manager software is installed.
2. On the **Apps** screen, in the **Avaya** section, select **License Manager Configuration**.
3. Select the **Configuration** tab.
4. On the License Manager Configuration Tool window, from the **License Type** list, select **Remote WebLM**.
5. In the **WebLM IP or Fully Qualified Domain Name** box, type the IP address or Fully Qualified Domain Name (FQDN) host name of the Avaya WebLM server.
6. Click **Apply**.
7. On the pop-up dialog, click **Yes** to restart Contact Center License Manager.
8. Click **Close** to close the window.

Part 3: Contact Center Manager Server Utility

- Access Class operations on page 92
- Connected user and user account operations on page 97
- Serial port configuration on page 108
- Server settings on page 110
- PABX configuration on page 111
- Alarm and Event configuration on page 112
- Voice Prompt Editor configuration on page 122

Chapter 9: Server Utility Access Class operations

The System Administrator establishes and maintains system security in a Contact Center. An access class is a defined set of privileges that specify login, read, and write permissions for a given resource. By assigning the appropriate Server Utility access classes to the appropriate users, the Administrator can help ensure system security. For example, you can restrict access to certain Server Utility components to senior administrators.

Server Utility access classes are different from CCMA access classes. For information on CCMA access classes, see *Avaya Aura® Contact Center Client Administration*.

Prerequisites to Contact Center Manager Server Utility access class operations

Procedure

Install and commission Server Utility. See *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.

Logging on to Server Utility

About this task

You must log on to the Server Utility to perform tasks relating to access classes.

The default login information for the Server Utility is as follows:

- User ID: sysadmin
- Password: avaya1

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Server Utility**.

2. On the **Avaya Contact Center Manager - Server Utility Login** dialog box, in the **User ID** box, type the user ID for the Contact Center Manager Server on which to log on.
3. In the **Password** box, type the password for the Contact Center Manager Server on which to log on.
4. From the **Server Name or IP address** list, select the Contact Center Manager Server name or IP address.
5. Click **OK**.

Creating an access class

Before you begin

- Log on to Server Utility. See Logging on to Server Utility on page 92.

About this task

Create an access class from the Server Utility window.

Procedure

1. In the Server Utility window, double-click **User Administration**.
2. Double-click **Access Classes**.
3. In the Access Classes window, choose **File** > **New**.
4. In the **New Access Class** dialog box, in the **Name** box, type a name for the access class.

   Use a descriptive name to describe the type of user having this access level or the type of privileges available at this access level.
5. In the **Comments** box, type additional optional information about the access class.
6. Click the **Access** tab.
7. On the **Access** tab, select a function to make available to this access class.

   The selected function appears in the Selected item box.
8. From the **Level of Access** list, select the desired level of access for that function.
9. Repeat step 7 on page 93 and step 8 on page 93 for each function to which you want this access class to have access.
10. Click **Save**.
11. To return to the Server Utility window, click **File** > **Close**.

Viewing members of an access class

Before you begin

- Log on to Server Utility. See Logging on to Server Utility on page 92.

About this task

View the members of an access class from the Server Utility window.

Procedure

1. From the Server Utility window, expand **User Administration**.
2. Double-click **Access Classes**.
3. In the **Access Classes** dialog box, select the access class for which you want to display the members.
4. Click **File** > **Properties**.
5. On the **Access Class Properties** dialog box, click the **Members** tab.
6. On the **Members** tab, you can see the members of the access class
7. To return to the Server Utility window, click **File** > **Close**.

Modifying access class properties

Before you begin

- Log on to Server Utility as a system administrator. See Logging on to Server Utility on page 92.
- Create the access classes to modify. See Creating an access class on page 93.

About this task

The System Administrator can modify access class properties if the default properties do not meet your users needs. You can modify the access permissions and the users for each access class. You cannot modify the name or the description of the default access class.

Procedure

1. In the Server Utility window, double-click **User Administration**.
2. Double-click **Access Classes**.
3. From the Access Classes window, select the access class to change.
4. Click **File** > **Properties**.
5. Click the **General** tab.
6. View the name and the description of the access class.
7. Click the **Access** tab.

8. On the **Access** tab, select a function to make available to this access class.

   The selected function appears in the Selected item box.
9. From the **Level of Access** list, select the level of access for that function.
10. Repeat step 8 on page 95 and step 9 on page 95 for each function to which you want this access class to have access.
11. Click the **Members** tab.
12. Add the members of the access class.
13. Click **Save**.
14. To return to the Server Utility window, click **File** > **Close**.

Previewing the list of access classes

Before you begin

- Log on to Server Utility. See Logging on to Server Utility on page 92.

About this task

Preview the list of available access classes to determine which access class provides a new user with the required level of accessibility.

Procedure

1. In the Server Utility window, double-click **User Administration**.
2. Double-click **Access Classes**.
3. From the Access Classes window, click **File** > **Print Preview**.
4. Select the **Print Preview Range**.
5. Click **Print Preview**.

   A window appears showing the current list of classes and assignments. You can print the list from the Print Preview window.

Variable definitions

Name	Description
Print Preview Range	Choose to print all of the access classes, or only the selected access class.

Printing the list of access classes

Before you begin

- Log on to Server Utility. See Logging on to Server Utility on page 92.

About this task

Print the list of available access classes for corporate records to determine which access class provides a new user with the required accessibility.

Procedure

1. In the Server Utility window, double-click **User Administration**.
2. Double-click **Access Classes**.
3. From the Access Classes window, click **File** > **Print**.
4. Select your printer and the printer properties.
5. Click **OK**.

Deleting an access class

Before you begin

- Log on to Server Utility. See Logging on to Server Utility on page 92.

About this task

Delete an access class that you no longer use.

Important:

You cannot delete the default access classes (“AdminGroup”, "Call Centre Admin", or “Supervisor”) or any access class that has members.

Procedure

1. In the Server Utility window, double-click **User Administration**.
2. Double-click **Access Classes**.
3. From the Access Classes window, select the access classes to delete, and click **File** > **Delete**.
4. In the Confirmation dialog box, click **Yes**.

Chapter 10: Connected user and user account operations

This chapter describes how to administer users who are currently connected to the server and their user accounts and privileges. A desktop user account uses the Server Utility application to access Contact Center Manager Server. You must create a desktop user account for each user who requires access to the server. You must also assign each account the access class that gives users the privileges they need to perform their job.

You can use the Server Utility to create desktop user accounts. Users can use these accounts to log on to the Server Utility, to access the server database, or to log on to a wallboard.

The Contact Center Administrator can use the Server Utility to create desktop user accounts with permission granted to select all data from the Historical Reporting views or real-time data. The administrator cannot configure desktop users as supervisors.

Prerequisites to Contact Center Manager Server Utility connected user operations

Procedure

- Install and commission Server Utility. See *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.
- Log on to Server Utility. See Logging on to Server Utility on page 92.

Viewing a list of connected users

About this task

Check the status of a connection to the server for a desktop user.

Procedure

1. From the Server Utility window, click **System Administration** > **System Configuration**.

2. Double-click **Connected Sessions**.

   The Connected Sessions window appears. This list displays the desktop users who are logged on to the server, their user IDs, their location (network address), and the time of their last activity on the system.

3. To return to the Server Utility window, choose **File** > **Close**.

Logging off a user

About this task

Immediately disconnect and log off a user. The disconnected user is not warned.

Procedure

1. From the Server Utility window, expand **System Administration** > **System Configuration**.
2. Double-click **Connected Sessions**.
3. In the Connected Sessions window, select the PC User ID of the user to disconnect.
4. Choose **File** > **Disconnect Session**.
5. In the message box that appears asking you to confirm your choice, click **Yes**.

   You return to the Connected Sessions window. The user is no longer on the list.

6. Click **File** > **Close**.

Setting privileges for a user

About this task

You can assign a variety of privileges to certain functions to provide users with the accessibility they need to successfully perform their job.

Procedure

1. For each access class, select the Contact Center Manager Server functions that members of that class can use in Server Utility.
2. Create desktop user accounts for users who require access to Contact Center Manager Server functions. See Adding desktop user accounts on page 103.
3. Assign access classes to user accounts, giving users the privileges they need to perform their jobs. See Changing the properties of a desktop user on page 106.

Procedure job aid

The following table describes the privileges assigned to functions in Server Utility.

Function	Privilege	Description
Access Classes	View	View the properties for any access class.
	Edit	View and modify properties for any access class.
	Create/Delete	View, modify, add, or delete access classes.
Activity Codes	View	View the properties for any activity codes.
	Edit	View and modify properties for any activity codes.
	Create/Delete	View, modify, add, or delete activity codes.
Agent Threshold Classes	View	View the properties for any agent threshold class.
	Edit	View and modify properties for any agent threshold class.
	Create/Delete	View, modify, add, or delete agent threshold class.
Agent to Skillset Assignments	View own agents only	View the properties for the agents configured in your group.
	View and assign own agents only	View the properties and assign skillsets for the agents configured in your group.
	View all agents	View the properties for all agents configured in the contact center.
	View and assign all agents	View the properties and assign skillsets for all agents configured in the contact center.
Agent to Supervisor Assignments	View own agents only	View the properties for the agents configured in your group.
	View and assign own agents only	View the properties and assign supervisors for the agents configured in your group.
	View all agents	View the properties for all agents configured in the contact center.
	View and assign all agents only	View the properties and assign supervisors for all agents configured in the contact center.
Alarm Monitor	View	View event details for system alarms.
	Create/Delete	View event details for system alarms, clear and acknowledge system alarms.
Application Threshold Classes	View	View the properties for any application threshold classes.
	Edit	View and modify properties for any application threshold class.
	Create/Delete	View, modify, add, or delete application threshold classes.
Applications	View	View the properties for any application.
	Edit	View and modify properties for any application.
Backup Scheduler	View	View the list of available backup schedules.

Table continues…

Function	Privilege	Description
	Edit	View and modify the properties of backup schedules.
	Create/Delete	View, modify, and delete backup schedules.
Call Presentation Classes	View	View the call presentation classes.
	Edit	View and modify the call presentation classes.
	Edit, Create/ Delete	View, modify, and delete the call presentation classes.
CDNs	View	View the call distribution numbers.
	Edit	View and modify the call distribution numbers.
	Edit, Create/ Delete	View, modify, and delete the call distribution numbers.
Connected Sessions	View	View the connected sessions window.
	Create/Delete	View the connected sessions and log off any connected users.
DNISs	View	View the dialed numbers.
	Edit	View and modify the dialed numbers.
	Create/Delete	View, modify, and delete the dialed numbers.
Emergency Help	View	View the emergency help configuration.
Event Browser	View	View all Informational, Critical, Minor, or Major events in the Event Browser.
Event Preferences	View	View event preferences configured for event codes.
	Edit	View event preferences and increase or decrease the severity.
	Create/Delete	Create event preferences, increase or decrease the severity, modify or delete event preferences.
Formulas	View	View formulas for statistical reports.
	Edit	View and modify formulas for statistical reports.
	Create/Delete	Create, modify, or delete formulas for statistical reports.
Historical Statistics	View	View historical statistics.
	Edit	View and modify historical statistics.
IVR ACD-DN Threshold Classes (Avaya Communication Server 1000)	View	View IVR ACD-DN Threshold Classes
	Edit	View and modify IVR ACD-DN Threshold Classes
	Create/Delete	Create and delete IVR ACD-DN Threshold Classes
IVR ACD-DNs (Avaya Communication Server 1000)	View	View IVR ACD-DNs.
	Edit	View and modify IVR ACD-DNs.
	Create/Delete	Create, modify, or delete IVR ACD-DNs.
Network Communication Parameters	View	View Network Communication Parameters.
	Edit	View and modify Network Communication Parameters.

Table continues…

Function	Privilege	Description
Network Historical Statistics (NCC)	View	View Network Historical Statistics.
	Edit	View and modify Network Historical Statistics.
Network Skillsets (NCC)	View	View network skillsets.
	Edit	View and modify network skillsets
	Create/Delete	Create and delete network skillsets.
Nodal Threshold Class	View	View nodal threshold classes.
	Edit	View and modify nodal threshold classes.
Phoneset Displays (Avaya Communication Server 1000)	View	View telephone displays.
	Edit	View and modify telephone displays.
Phonesets	View	View telephones.
	Edit	View and modify telephones.
	Create/Delete	Create and delete telephones.
Real-Time Displays	View own agents	View your agents in real-time displays.
	View own agents–create displays	View your agents in real-time displays and create displays.
	View all agents	View all agents in real-time displays.
	View all agents–create displays	View all agents in real-time displays and create displays.
Real-time Statistics	View	View real-time statistics.
	Edit	View and modify real-time statistics.
Reports	Create and run any report	Create and run any report.
Reports–Agent Performance	Create and run any report	Create and run Agent Performance reports.
Reports–Call by Call	Create and run any report	Create and run Call by Call reports.
Reports–Other	Create and run any report	Create and run Other reports.
Route Threshold Classes (Avaya Communication Server 1000)	View	View route threshold classes.
	Edit	View and modify route threshold classes.
	Create/Delete	Create and delete route threshold classes.
Routes (Avaya Communication Server 1000)	View	View routes.
	Edit	View and modify routes.
	Create/Delete	Create and delete routes.
Scheduler	View	View the scheduler.

Table continues…

Function	Privilege	Description
	Edit	View and modify the scheduler.
	Create/Delete	Create and delete the scheduler.
Script Variables	View	View script variables.
	Edit	View and modify script variables.
	Create/Delete	Create and delete script variables.
Scripts	View	View scripts.
	Edit	View and modify scripts.
	Create/Delete	Create and delete scripts.
Serial Ports	View	View the Serial Ports window and properties for all serial ports.
	Edit	View the Serial Ports window and view and modify properties for all serial ports.
Server Performance Monitor	View	View the Server Performance Monitor.
Server Settings	View	View detailed information about the server, such as the software release and the serial number.
Sites (NCC)	View	View sites on the NCC.
	Edit	View and modify sites on the NCC.
	Create/Delete	Create and delete sites on the NCC.
Skillset Threshold Classes	View	View skillset threshold classes.
	Edit	View and modify skillset threshold classes.
	Create/Delete	Create and delete skillset threshold classes.
Skillsets	View	View skillsets.
	Edit	View and create skillsets.
	Create/Delete	Create and delete skillsets.
Switch Resource	View	View the PABX Resource properties for the telephony PABX type.
	Edit	Users can view and modify the PABX Resource properties.
Table Routing Assignments (NCC)	View	View table routing assignments.
	Edit	View and modify table routing assignments.
	Create/Delete	Create and modify table routing assignments.
Users	View reporting agents only	View the Users window and view properties for reporting agents.
	View and edit reporting agents only	View the Users window and view and modify properties for reporting agents.

Table continues…

Function	Privilege	Description
	Edit all agents–create agents only	View the Users window and view, modify, create, and delete any agents.
	View all users	View the Users window and view properties for all desktop users, supervisors, and agents. Users require this access privilege to generate call-by-call reports.
	Edit all users	View the Users window and view and modify properties for all desktop users, supervisors, and agents.
	Edit all users–create any type	View the Users window and view, modify, add, and delete desktop users, supervisors, and agents.
Voice Ports	View	View the Voice Ports window and view properties for all voice ports.
	Edit	View the Voice Ports window and view and modify properties for all voice ports.
Voice Prompt Editor	View	Log on to the Voice Prompt Editor and view voice files and voice segments.
	Edit	Log on to the Voice Prompt Editor and view and modify voice segments and voice files.
	Create/Delete	Log on to the Voice Prompt Editor and view, modify, add, and delete voice files and voice segments. In Avaya CallPilot®, use Application Builder to work with voice prompts.

Adding desktop user accounts

Before you begin

- Create at least one access class. See Creating an access class on page 93.

About this task

Use Server Utility to add a desktop user account permissions and accessibility to the features of the Contact Center Manager Administration application.

Avaya recommends that you add new users to create Data Source Names (DSN) for Expert reports. For more information on Expert reports, see *Using Avaya Aura® Contact Center Reports and Displays*.

If adding a new desktop user account in a contact center that uses the High Availability feature, the new user is not created automatically on the standby server. To copy the user account to the standby server, you must perform one of the following tasks:

- Back up the active server database and restore it on the standby server.
- Manually create the account on the standby server. Create the account using the same details as used on the active server.

Procedure

1. On the Server Utility window, double-click **User Administration** and then double-click **Users**.
2. In the **Users** dialog box, choose **File** > **New**.
3. In the **New User** dialog box, on the **General** page, enter the contact information for the user.
4. Click the **Desktop** tab.
5. On the **Desktop** page, in the **User ID** box, type a user ID.

   Important:

   The desktop user uses this to log on to the server. You cannot change the user ID after you save the user account.
6. Click **Set Password**.
7. In the **Set Password** dialog box, in the **New Password** and **Confirm Password** boxes, type the password.

   If you open an existing desktop user, this button appears as **Reset Password**.
8. Click **OK**.

   The Set Password window closes.
9. Select the **Password Expires** check box to indicate that the password expires in 180 days.

   For special users, such as wallboard displays used with third-party software, you can leave the check box clear so that password never expires. The administrator password does not expire.
10. From the **Access Class** list, select the access class to which to assign the user.
11. Click **Save** to save your settings and return to the Users window.
12. Click **File** > **Close**.

Preventing users from accessing the server

Before you begin

- Log off the desktop user. See Changing the properties of a desktop user on page 106.

About this task

You can restrict the access for desktop users who do not have the authority, knowledge, or responsibility to update the server settings.

Procedure

1. On the Server Utility window, double-click **User Administration**, and then double-click **Users**.
2. In the **Users** dialog box, double-click the user name.
3. In the **User Properties** dialog box, click the **Desktop** tab.
4. On the **Desktop** page, click **Lock Out**.

   The user desktop status changes to Locked out by an administrator. This continues to be the current status of the user until an administrator restores it to OK. The Lock Out button changes to Restore.
5. Click **Save**.
6. Choose **File** > **Close**.

Restoring access to the server for a user

About this task

Restore or grant access for a desktop user on the server. You can grant access for specific periods of time.

Perform this procedure when a user is locked out of the system after exceeding the password retry count or after an administrator manually locks out a user.

Procedure

1. On the Server Utility window, double-click **User Administration**, and then double-click **Users**.
2. In the **Users** dialog box, double-click the user name.
3. In the **User Properties** dialog box, click the **Desktop** tab.
4. On the **Desktop** page, click **Restore**.

   The user desktop status changes to OK. The Restore button changes to Lock Out.
5. Click **Save**.
6. Choose **File** > **Close**.

Resetting desktop passwords

Before you begin

- Log on to Server Utility as sysadmin.

About this task

Reset desktop passwords when users forget their desktop password or if the desktop password expires.

By resetting the password, you can create a new password for the desktop user.

The desktop user password expires after 180 days unless the user changes the password within that time. Seven days before the expiry of the password, the Server Utility displays a warning message during the user logon.

If users want to change their password, they can log on to the server and click Utilities, Change Password.

Procedure

1. On the Server Utility window, double-click **User Administration**, and then double-click **Users**.
2. In the **Users** dialog box, double-click the user name.
3. In the **User Properties** dialog box, click the **Desktop** tab.
4. On the **Desktop** page, click **Reset Password**.
5. On the **Reset Password** dialog box, in the **New Password** and **Confirm New Password** boxes, type the new password.
6. Click **OK** to close the **Reset Password** dialog box.
7. Click **Save**.
8. Click **File** > **Close**.

Changing the properties of a desktop user

Before you begin

- To change the access class of a particular user, ensure that the user is not logged on.

  Important:

  If the user is logged on, the server logs the user off when you change their properties.

About this task

Change the properties of a desktop user if the default properties are not sufficient.

Procedure

1. On the Server Utility window, double-click **User Administration**, and then double-click **Users**.
2. In the **Users** dialog box, double-click the desktop user to change.
3. In the **User Properties** dialog box, make any required changes.

4. Click **Save** to save your changes.

Deleting a desktop user

Before you begin

- Ensure the user to be deleted is logged off, otherwise, the user is immediately logged off without warning.

Important:

When the desktop user is removed, the system logs out the user without warning even if the user is logged in.

About this task

Delete a desktop user if that user no longer requires access to the server.

Procedure

1. On the Server Utility window, double-click **User Administration** and then double-click **Users**.
2. From the Users window, select the desktop user to delete.
3. Click **File** > **Delete**.
4. Click **OK**.

Chapter 11: Serial port configuration

Serial ports are input/output devices used to connect external equipment, such as modems, to your computer. Serial ports transmit data from these external devices one bit at a time.

You can use the Serial Ports window to view or edit serial port settings. From this window, you can modify a serial port baud rate, data bits, stop bits, parity, and flow control. You can also use the Serial Port Properties page to edit serial port settings.

Prerequisites to Contact Center Manager Server Utility serial port configuration

Procedure

- Install and commission Server Utility. See *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.
- Log on to Server Utility. See Logging on to Server Utility on page 92.

Viewing port settings

About this task

View the Serial Ports window to ensure the accuracy of the port settings.

Procedure

1. In the Server Utility window, expand **System Administration**.
2. Expand **System Configuration**.
3. Double-click **Serial Ports**.
4. On the Serial Ports window, select a configured serial port.
5. Click **File** > **Properties**.

Editing port settings

About this task

You can use the Serial Ports window to modify serial port settings, such as baud rate, data bits, stop bits, panity, and flow control.

Procedure

1. In the Server Utility window, expand **System Administration**.
2. Expand **System Configuration**.
3. Double-click **Serial Ports**.
4. On the Serial Ports window, select a configured serial port.
5. Click **File** > **Properties**.
6. Configure the changes to the properties of the Serial Port.
7. Click **Save**.

Chapter 12: Server settings

This chapter describes how to view detailed information about Contact Center Manager Server resources. This information is saved to the server database during installation and can be retrieved for technical support purposes.

Prerequisites to Contact Center Manager Server Utility server settings

Procedure

- Install and commission Server Utility. See *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.
- Log on to Server Utility. See Logging on to Server Utility on page 92.

Viewing server resources

About this task

You can view detailed information about the server resources, such as the software release number and the serial number. You can also view a list of services and features installed on your system.

Procedure

1. Log on to the server where the Server Utility is installed.
2. On the **Apps** screen, in the **Avaya** section, select **Server Utility**.
3. On the Server Utility window, expand **System Administration.**
4. Expand **System Configuration**.
5. Double-click **Server Settings**.

Chapter 13: PABX configuration

You can record information about an Avaya Communication Server 1000 PABX after initial software installation.

Prerequisites to Contact Center Manager Server Utility PABX configuration

Procedure

Install and commission Server Utility. See *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.

Recording PABX information

About this task

Record PABX information using the PABX Resource property sheet after the initial software installation. You can record the PABX type, subtype, and release number. Depending on the PABX type, some fields are not applicable and therefore are blank.

Procedure

1. Log on to the **Server Utility**.
2. From the Server Utility window, double-click **System Administration**.
3. Double-click **System Configuration**.
4. Double-click **Switch Resource**.
5. Ensure the **Switch Type** and **Switch Subtype** are correct.
6. Record the **Customer Number**, **Name**, and **IP Address**.
7. Click **Close**.

Chapter 14: Alarm and Event configuration

The Event Browser and Alarm Monitor show events that occur on the Contact Center Manager Server. These programs provide many common features for viewing events. The following table provides more information about these features:

Table 1: Event Browser versus Alarm Monitor features

Feature	In Event Browser?	In Alarm Monitor?
View events	Yes	Yes
View online Help for an event	Yes	Yes
Sort events by category	Yes	Yes
Save a list of events	Yes	No
Print a list of events	Yes	Yes
View minor, major, critical events	Yes	Yes
View information events	Yes	No
Filter events by code, type, severity, most recent events	Yes	No
Filter events using Event Preferences graphical user interface	Yes	Yes
Automatically show the graphical user interface in the foreground when an event occurs	No	Yes
Clear an event	No	Yes

Event Browser

Events are log entries that record activities in Contact Center Manager Server, such as sending or receiving messages, opening or closing applications, and errors. Some events are for information only, while others can indicate problems. You can filter events by several categories, such as severity and event code range. You can also limit the display to the most recent events.

Alarm Monitor

The Alarm Monitor automatically appears in the foreground of the desktop when an event occurs, alerting the Administrator to problems. You can specify whether the Alarm Monitor appears in the foreground for only critical events, major and critical events, or all events, or whether it stays in the background.

In the Alarm Monitor, you can filter events by severity only. The Alarm Monitor does not display information events.

Prerequisites to Event Browser configuration

Procedure

- Install and commission Server Utility. See *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.
- Log on to Server Utility. See Logging on to Server Utility on page 92.

Starting the Event Browser from Server Utility

Before you begin

- Log on to Server Utility. See Logging on to Server Utility on page 92.

About this task

You can start the Event Browser from the Server Utility.

Procedure

1. On the Server Utility window, expand **System Administration**.
2. Expand **Alarms & Events**.
3. Double-click **Event Browser**.

Sorting events in the Event Browser

Before you begin

- Open the Event Browser. See Starting the Event Browser from Server Utility on page 113.

About this task

You can sort events based on time, event code, event type, severity, and object ID.

Procedure

On the Event Browser window, click the header of the column by which you want to sort.

Viewing online Help for an event

Before you begin

- Open the Event Browser. See Starting the Event Browser from Server Utility on page 113.

About this task

View online Help for a selected event. The online Help displays the code, severity, description, impact, and recovery action of the event. The listed recovery actions can provide a recommended action to correct the problem or additional information about the event.

Procedure

1. In the Event Browser, select the event to you want to investigate.
2. Click **Help on Event**.

Saving a list of events

Before you begin

- Ensure the filter settings are configured to show the type and number of events to save. See Changing the filtering criteria for events on page 114.
- Open the Event Browser. See Starting the Event Browser from Server Utility on page 113.

About this task

Save relevant sections of the event log in case of a problem with your system. The log helps technical support representatives to analyze your system.

Procedure

1. From the Event Browser window, click **File** > **Save Event Log**.
2. In the **Save As** dialog box, click a save range.
3. Click **OK**.
4. In the dialog box that appears, enter a recognizable file name and location.
5. Click **Save**.
6. In the **Confirmation** dialog box, click **OK**.

Changing the filtering criteria for events

Before you begin

- Open the Event Browser. See Starting the Event Browser from Server Utility on page 113.

About this task

Change the filter criteria for events so that you can either view every single event that arises or specify which event types to view. By changing the filtering criteria, you can reduce the number of events shown at one time and force the Event Browser to display only the events in which you are interested.

You can configure the event log filter to display the following:

- a specific number of most recent events, or all events (all events available on or retrieved from the system)
- events of a certain severity (critical, major, minor, information)
- a specific event code range or all event codes
- a specific type of alarm (alarm set, alarm cleared, or message)
- events that occurred during a specific date and time interval

Procedure

1. Click **File** > **Change Filter criteria**.
2. In the **Set Event Filter Properties** dialog box, on **Report and Severity** tab, select the **All events** or **Latest** option.
3. If you select the **Latest** option. indicate the number of most recent events you want to view.
4. Select the **Severity** check boxes that indicate the type of events you want to view: **Critical, Major, Minor**, **Information**.
5. Click the **Code and Type** tab.
6. On the **Code and Type** page, select the **All Codes** or **Code Range** option.
7. If you select the **Code Range** option, indicate the minimum and maximum code range to view.
8. Select all of the **Type** check boxes that interest you: **Alarm Set, Alarm Cleared,** and **Message**.
9. Select the **Interval** tab.
10. To view all events, enable **First Event** and **Last Event**. To filter events, select a **Start Time** and **End Time**.
11. Click **OK** to change the filter.

Adding an event preference

Before you begin

- Open the Event Browser. See Starting the Event Browser from Server Utility on page 113.

About this task

Add an event preference to override the default severity or throttling parameters of any event code. For example, you can change the preferences of an event to one of the following:

- Increase the severity of an event (for example, from Information to Minor). By increasing an event severity, you ensure that the event appears in the Alarm Monitor when it occurs.

- Reduce the severity of a recurring alarm to Information. By reducing an event severity, you prevent it from appearing in the Alarm Monitor.
- Configure the limiting parameters to reduce the frequency with which an event is logged.

Previous occurrences of the event are not affected. You can revert to the default event definition at any time by deleting the event preference for that event code.

Procedure

1. On the Server Utility window, expand **System Administration**.
2. Expand **Alarms & Events**.
3. Double-click **Event Preferences**.
4. From the Event Preferences window, click **File** > **New**.
5. In the **New Event Preference Properties** dialog box, in the **Event Code** box, type the event code number for the event to add.

   Important:

   Contact Center Manager Server does not accept unrecognizable event codes. For a complete list of valid event codes, refer to the Event Browser section and select Event Code Reference from the Help menu.
6. From the **Severity** list, select the severity to assign to the event.
7. In the **Interval** box, type the throttling interval.
8. In the **Threshold** box, type the number of instances of the event that can be logged during the specified interval.
9. Click **Save** to return to the Event Preferences window.
10. Click **File** > **Close**.

Variable definitions

Name	Description
Interval	The time interval during which the event can be logged a specified number of times. For example, in 30 minutes (the interval), log the event a maximum of 10 times (the number).

Throttling all events

Before you begin

- Open the Event Browser. See Starting the Event Browser from Server Utility on page 113.

About this task

Use event throttling to control the frequency with which events are recorded by the server log. You can limit all events to prevent the log from becoming overcrowded. If too many instances of each event are recorded, the log might have insufficient space to record more important events. Too many instances of the same event can distract users, causing them to overlook other important events.

Procedure

1. From the Server Utility window, expand **System Administration**.
2. Expand **Alarms & Events**.
3. Double click **Event Preferences**.
4. From the Event Preferences window, click **File** > **Default Throttling**.
5. In the **Set Default Throttling Properties** dialog box, select the **Enable** check box.
6. In the **Interval** box, type the interval for which you want to configure throttling.
7. In the **Number** box, type the number of instances of each event that you want logged.
8. Click **Save** to return to the Event Preferences window.
9. Click **File** > **Close**.

Changing an event preference

Before you begin

- Open the Event Browser. See Starting the Event Browser from Server Utility on page 113.

About this task

Change an event preference if one is already defined for the event. You can change the event severity.

Procedure

1. From the **Server Utility** window, expand **System Administration**.
2. Expand **Alarms & Events**.
3. Double click **Event Preferences**.
4. From the **Event Preferences** window, select an event preference to change.
5. Click **File** > **Properties**.

Deleting an event preference

Before you begin

- Open the Event Browser. See Starting the Event Browser from Server Utility on page 113.

About this task

Remove an event preference from the system. The event settings for severity and throttling revert to default values.

Procedure

1. From the Event Preferences window, select the event preference to delete.
2. Click **File** > **Delete**.

Changing the classification of an event

Before you begin

- Open the Event Browser. See Starting the Event Browser from Server Utility on page 113.

About this task

Change the default classification of particular events. For example, you can choose to treat a major event as a minor event if you are aware that the event is being resolved.

Procedure

1. Click **File** > **Change Filter Criteria**.
2. In the **Set Event Filter Properties** dialog box, select the desired criteria on all tabs.

Opening the Alarm Monitor

Before you begin

- Log on to Server Utility. See Logging on to Server Utility on page 92.

About this task

The Alarm Monitor appears in the foreground when a critical, major, or minor event occurs. If you cannot see the Alarm Monitor or if it is closed, follow this procedure to open the Alarm Monitor.

Procedure

1. On the Server Utility window, expand **System Administration**.
2. Expand **Alarms & Events**.
3. Double-click **Alarm Monitor**.

Refreshing the Alarm Monitor

Before you begin

- Open the Alarm Monitor. See Opening the Alarm Monitor on page 118.

About this task

Refresh the Alarm Monitor window any time to ensure you view the most complete list of alarms.

Important:

After you refresh the Alarm Monitor, the number of alarms can decrease. Alarms cleared by other processes are removed from the Alarm Monitor.

Procedure

From the Alarm Monitor window, click **View** > **Refresh**.

Sorting events in the Alarm Monitor

Before you begin

- Open the Alarm Monitor. See Opening the Alarm Monitor on page 118.

About this task

Sort events in the Alarm Monitor to review particular timestamp, severity, or information level.

Procedure

From the Alarm Monitor window, click the header of the column by which to sort.

Important:

By default, events are sorted by timestamp in reverse chronological order, the most recent appears at the top of the list.

Specifying when the Alarm Monitor appears in the foreground

Before you begin

- Log on to Server Utility. See Logging on to Server Utility on page 92.

About this task

The Alarm Monitor appears in the foreground when any event occurs, it takes the Windows desktop focus from the currently active window. You can configure the severity of alarm that forces the Alarm Monitor to appear in the foreground.

Procedure

1. On the Server Utility window, click **Utilities**.
2. Select the menu item that meets your criteria for when you want to be alerted about new alarms.

Procedure job aid

In the Server Utility window, from the **Utilities** menu, choose one of the following options:

- **Alert All Alarms**: show the Alarm Monitor window every time an alarm is registered or updated.
- **Alert Major and Critical Only**: show the Alarm Monitor window every time a Major or Critical alarm is registered or updated.
- **Alert Critical Only**: show the Alarm Monitor window every time a Critical alarm is registered or updated.

Configuring the Alarm Monitor to appear in the background

Before you begin

- Log on to Server Utility. See Logging on to Server Utility on page 92.

About this task

If you do not want to see the Alarm Monitor every time it receives and updates a new alarm, you can force it to appear in the background.

Procedure

On the Server Utility window, click **Utilities** > **Alerting Off**.

The Alarm Monitor moves to the background. When a critical alarm is registered, the Alarm Monitor window taskbar flashes until you move the Alarm Monitor window to the foreground.

Obtaining more information about an alarm

Before you begin

- Open the Alarm Monitor. See Opening the Alarm Monitor on page 118.

About this task

Obtain additional details about a specific alarm at any time after it appears in the Alarm Monitor window.

Procedure

1. On the Alarm Monitor window, double-click an alarm entry.
2. In the **Events Details** dialog box, click **Help on Event**.

Manually clearing an alarm

Before you begin

- Open the Alarm Monitor. See Opening the Alarm Monitor on page 118.

About this task

Clear an alarm to remove the selected alarm (but not the event that raised it) from the event log. This action also removes the selected alarm from the list in the Alarm Monitor. If the event occurs again, however, the alarm reappears in the Alarm Monitor.

Important:

Contact Center Manager Server automatically clears alarms when the alarm condition changes.

Procedure

1. On the Alarm Monitor window, select the alarm to clear it.
2. On the **Alarm Monitor**, choose **File** > **Clear Alarm**.
3. In the **Clear Alarm** dialog box, click **Yes** to confirm clearing of the selected alarm.

Chapter 15: Voice Prompt Editor configuration

To create and manage voice files and voice prompts for Contact Center Voice Services, you must log on to the Voice Prompt Editor.

The Voice Prompt Editor is available only if you use one of the following applications:

- Contact Center Voice Services on Avaya CallPilot®
- Application Builder to manage your voice prompts

Prerequisites to Voice Prompt Editor procedures

Procedure

Ensure that you are connected to Avaya Communication Server 1000.

Logging on to the Voice Prompt Editor

Before you begin

- Log on to Server Utility. See Logging on to Server Utility on page 92.

About this task

Log on to the Voice Prompt Editor to create and manage voice files and voice prompts.

Procedure

1. From the Server Utility window, expand **System Administration**, **System Configuration**.
2. Double-click **Voice Prompt Editor**.
3. In the **Account** box, type the mailbox containing the voice prompts with which to work.
4. In the **Password** box, type the password for that mailbox.
5. In the **Telephone No.** box, type the phone number of the phone to use to record or play back voice segments.

6. Click **Login**.

Logging off the Voice Prompt Editor

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.

About this task

Exit the Voice Prompt Editor.

Procedure

1. To log off the Voice Prompt Editor, choose **File** > **Logoff**.
2. Click **OK** to confirm that you want to log off.

   You are logged off the current session, open voice files are closed, and the Voice Prompt Editor Login window appears.
3. To exit completely, choose **File** > **Exit**.

Creating a voice file

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.

About this task

Organize your voice segments into a voice file.

Procedure

1. From the Voice Prompt Editor window, choose **File** > **New**.
2. In the **File Name** box, type the name of the new voice file. Voice file names are case-sensitive. When you reference voice files in scripts and variables, make sure the file name matches the name you create here.
3. In the **Subject** box, type an optional description of the new voice file.
4. To save the file, click **File** > **Save**.

Opening a voice file

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.

About this task

Open a voice file to display a list of voice segments stored in the selected voice file.

Procedure

1. From the Voice Prompt Editor window, choose **File** > **Open**.
2. In the **Open Voice File** dialog box, select the file to open.
3. Click **OK**.

   You return to the Voice Prompt Editor window. The window contains the list of segments in the selected voice file.

Reverting to a previously saved voice file

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.
- Open a voice file and make changes to it. See Opening a voice file on page 124.

About this task

If you change a voice file and then decide that you do not want to keep the changes, you can restore the previous copy of the voice file.

Procedure

From the Voice Prompt Editor window, choose **File** > **Revert**.

Copying a voice file

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.
- Ensure that the voice file is closed.

About this task

Copy a voice file.

Procedure

From the Voice Prompt Editor window, choose **File** > **Copy**.

Renaming a voice file

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.
- Ensure that the voice file is closed.

About this task

Rename a voice file.

Procedure

From the Voice Prompt Editor window, choose **File** > **Rename**.

Deleting a voice file

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.
- Ensure that the voice file is closed.

About this task

You can delete a voice file.

The voice file is not deleted until you log off the Voice Prompt Editor. Until then, you can restore any voice file that you mark for deletion.

Procedure

From the Voice Prompt Editor window, choose **File** > **Delete**.

Restoring a voice file

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.
- Ensure that the voice file is closed.

About this task

If you delete a voice file, you can restore it, provided that you did not log off the Voice Prompt Editor since you marked the file for deletion.

Procedure

From the Voice Prompt Editor window, choose **File** > **Delete**.

Creating a voice segment

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.
- Open a voice file. See Opening a voice file on page 124.

About this task

Create voice segments to add to voice files.

Procedure

1. In the Voice Prompt Editor window, in the **Voice Segment** box, click **New**.
2. In the **New Voice Segment** dialog box, in the **Name** box, type the name of the new voice segment.
3. In the **Title** box, type a description for the new voice segment.
4. In the **Script** box, type the text that the new segment is to contain (This is for reference only).
5. Click **OK**.

   The New Voice Segment dialog box closes and the new segment is created.

Recording a voice segment

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.
- Create a voice segment. See Creating a voice segment on page 126.

About this task

After you create voice segment file, you can record a voice segment.

Procedure

1. In the Voice Prompt Editor window, select the voice segment to record.
2. Click the **Record** icon.

   The phone that you specified during log on rings.
3. Answer the phone.
4. After the tone, record the message for the voice segment.
5. Click the **Stop** icon.
6. Hang up.
7. To record another segment, repeat step 2 on page 126 to step 6 on page 126.

8. Select **File** > **Save** to save the new voice segments.

   Important:

   You must save all new voice segments to the server before you close the Voice Prompt Editor.

Playing a voice segment

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.
- Create a voice segment. See Creating a voice segment on page 126.
- Record a voice segment. See Recording a voice segment on page 126.

About this task

Play back a voice segment to hear what the customer hears when the voice segment is played.

Procedure

1. In the Voice Prompt Editor window, select the voice segment to play.
2. Click the **Play** icon.

   If the phone that you specified during log on is on-hook, it rings. If the phone is off-hook, the segment starts to play.
3. If the phone is on-hook, answer the phone.

   The segment starts to play.
4. To move the voice segment backward by 5 seconds, click the **Skip Backward** icon.

   OR

   To move the voice segment forward by 5 seconds, click the **Skip Forward** icon.
5. To play the next voice segment in the **Voice Segment** list, click the **Play Next** icon.
6. To stop, click the **Stop** icon.
7. Hang up.

Playing a group of voice segments

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.
- Create a voice segment. See Creating a voice segment on page 126.

- Record a voice segment. See Recording a voice segment on page 126.

About this task

Play a group of voice segments after you record them to see how they fit together and to determine if you need to adjust the silence in any segment.

Procedure

1. In the Voice Prompt Editor window, click **Group**.
2. In the **Edit Play Group** dialog box, from the **Voice Segments** list, select a voice segment to add to the play group.
3. Click **Add**.

   The voice segment is added to the Play Group list.
4. Repeat step 2 on page 128 to step 3 on page 128 until the voice segments that you need appear in the play group.
5. To remove a voice segment from the group, in the **Play Group** list, click the voice segment and then click **Remove**.
6. Click **Play**.
7. To move a voice segment up or down, in the **Play Group** list, click the voice segment and then click **Up** or **Down**.
8. When you finish playing the group, click **Stop**.
9. Click **Close** to return to the Voice Prompt Editor window.

Searching for a voice segment

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.
- Create a voice segment. See Creating a voice segment on page 126.
- Record a voice segment. See Recording a voice segment on page 126.

About this task

Search for a voice segment by its segment ID or by one or more of the following elements:

- the name of the voice segment
- the title of the voice segment
- the words used in the voice segment (as specified in the Script box)
- the duration of the voice segment

Procedure

1. In the Voice Prompt Editor window, click **Search**.

2. In the **Search for Segment** dialog box, click **Segment ID**.
3. In the **Segment ID** box, type the ID number of the voice segment.
4. To search on name, title, script, or duration, click **Text Fields**.
5. In the **Name**, **Title**, **Script**, or **Duration** boxes, type the text to find.
6. Click **Find Next**.
7. Click **Find Next** again to find the next segment that satisfies the search conditions.
8. When you finish, click **Cancel** to close the **Search for Segment** dialog box.

Lengthening or shortening a voice segment

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.
- Create a voice segment. See Creating a voice segment on page 126.
- Record a voice segment. See Recording a voice segment on page 126.

About this task

After you record a voice segment, you can lengthen or shorten the voice segment by modifying the beginning and ending of the segment.

Procedure

1. In the Voice Prompt Editor window, select the voice segment.
2. Click **Length**.
3. In the **Edit Length for Current Segment** dialog box appears, select the **Edit Length at** option.
4. Select the **Beginning with** check box.
5. To remove voice, noise, or silence from the beginning of the voice segment, from the **Beginning with** list, select a negative number of milliseconds.

   OR

   To add voice, noise, or silence to the beginning of the voice segment, from the **Beginning with** list, select a positive number of milliseconds.
6. Select the **End with** check box.
7. To remove voice, noise, or silence from the end of the voice segment, from the **End with** list, select a negative number of milliseconds.

   OR

   To add voice, noise, or silence to the end of the voice segment, from the **End with** list, select a positive number of milliseconds.

8. Click **Apply**.

   The Edit Length for Current Segment dialog box closes, and the voice segment is shortened or lengthened.

Removing all silence from a voice segment

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.
- Create a voice segment. See Creating a voice segment on page 126.
- Record a voice segment. See Recording a voice segment on page 126.

About this task

You can remove all silence from the beginning and ending of a specified voice segment. Silence in the middle of the voice segment is not removed.

Procedure

1. In the Voice Prompt Editor window, select the voice segment.
2. Click **Length**.
3. In the **Edit Length for Current Segment** dialog box, select the **Normalize** check box.
4. To remove all voice, noise, or silence from the beginning of the voice segment, select the **Beginning of Segment** check box.
5. To remove all voice, noise, or silence from the end of the voice segment, select the **End of Segment** check box.
6. Click **Apply**.

   The Edit Length for Current Segment dialog box closes, and all silence is removed from the beginning or end of the voice segment, or from both.

Removing or adding a specified length to all voice segments

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.
- Create a voice segment. See Creating a voice segment on page 126.
- Record a voice segment. See Recording a voice segment on page 126.

About this task

You can remove or add voice, silence, or noise to all voice segments.

Procedure

1. From the Voice Prompt Editor window, choose **File** > **Length**.
2. In the **Edit Segment Lengths in Voice File** dialog box, select **Edit Length at**.
3. Select the **Beginning with** check box.
4. To remove voice, noise, or silence from the beginning of the voice segments, from the **Beginning with** list, select a negative number of milliseconds.

   OR

   To add voice, noise, or silence to the beginning of the voice segments, from the **Beginning with** list, select a positive number of milliseconds.
5. Select the **End with** check box.
6. To remove voice, noise, or silence from the end of the voice segments, from the **End with** list, select a negative number of milliseconds.

   OR

   To add voice, noise, or silence to the end of the voice segments, from the **End with** list, select a positive number of milliseconds.
7. Click **Apply**.

   The Edit Segment Lengths in Voice File dialog box closes, and all voice segments are lengthened or shortened.

Removing all silence from all voice segments

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.
- Create a voice segment. See Creating a voice segment on page 126.
- Record a voice segment. See Recording a voice segment on page 126.

About this task

Remove all silence from all voice segments at one time.

Procedure

1. From the Voice Prompt Editor window, choose **File** > **Length**.
2. In the **Edit Segment Lengths in Voice File** dialog box, select the **Normalize** option.
3. To remove voice, noise, or silence from the beginning of the voice segment, select the **Beginning of Segment** check box.
4. To remove voice, noise, or silence from the end of the voice segment, select the **End of Segment** check box.

5. Click **Apply**.

   The Edit Segment Lengths in Voice File dialog box closes, and all silence is removed from the beginning or end of all voice segments.

Deleting a voice segment

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.
- Create a voice segment. See Creating a voice segment on page 126.
- Record a voice segment. See Recording a voice segment on page 126.

About this task

You can delete voice segments. The voice segment is not deleted until you close the voice file or log off the Voice Prompt Editor. Until then, you can restore any voice segments that you mark for deletion.

Procedure

1. In the Voice Prompt Editor window, from the **Voice Segment** list, click the voice segment.
2. Click **Delete**.

   The deletion mark (**d**) appears beside the selected voice segment.

Restoring a voice segment marked for deletion

Before you begin

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor on page 122.
- Create a voice segment. See Creating a voice segment on page 126.
- Record a voice segment. See Recording a voice segment on page 126.

About this task

If you delete a voice segment and then decide you do not want to delete it, you can cancel the deletion, provided that you did not close the voice file since deleting the segment.

Procedure

1. In the Voice Prompt Editor window, click the voice segment marked for deletion.
2. Click **Undo**.

   The deletion mark (**d**) disappears from beside the selected voice segment.

Part 4: Contact Center Manager Administration

- Contact Center Manager Administration configuration on page 134
- Avaya Communication Server 1000 Data Extraction Tool operation on page 155
- Language support fundamentals on page 164

Chapter 16: Contact Center Manager Administration configuration

The Contact Center Manager Administration server is the location of the configuration of the main controls for your Avaya Aura® Contact Center. Use the Contact Center Manager Administration application to configure servers, agents, supervisors, skillsets, route points, and many other tools for routing contacts to agents.

For procedures to add, change, and delete items from the Contact Center Manager Administration database, see the Contact Center Manager Administration online Help and *Avaya Aura® Contact Center Client Administration*.

The procedures in this chapter refer to any configuration items that you must perform on the server, outside of the Contact Center Manager Administration Client application.

Prerequisites to Contact Center Manager Administration configuration

Procedure

Commission Contact Center Manager Administration. See *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.

Configuring your logon warning message title and text

Before you begin

- Ensure that you have administrator privileges on the Contact Center Manager Administration server.

About this task

You can customize a warning message that appears when users attempt to log on to the Contact Center Manager Administration server. By default, this feature is enabled in the Contact Center Manager Administration software, however the message is not visible unless you configure your message title and text in the Local Security Policy tool of Windows Server 2012 Release 2.

If you have a domain security policy in place with a logon warning message configured, you cannot change the logon warning message using this procedure. In this case, you must contact your administrator to change the logon warning message.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. On the **Start** screen, click **Administrative Tools** > **Local Security Policy**.
3. In the Local Security Settings window, in the left pane, navigate to **Local Policies** > **Security Options**.
4. In the right pane, in the list of **Security Options**, right-click **Interactive logon: Message title for users attempting to log on** and select **Properties**.
5. In the **Interactive Logon** dialog box, in the **Interactive logon** box, type your message title.
6. Click **Apply**.
7. Click **OK**.
8. In the list of **Security Options**, right-click **Interactive logon: Message text for users attempting to log on** and select **Properties**.
9. In the **Interactive Logon** dialog box, in the **Interactive logon** box, type your warning message.
10. Click **Apply**.
11. Click **OK**.
12. Close all windows to complete the procedure.
13. If the Contact Center Manager Server is part of a networked contact center, configure this setting on each Contact Center Manager Administration server.

Enabling the logon warning message

Before you begin

- Ensure that you have administrator privileges on the Contact Center Manager Administration server.
- Configure your logon warning message title and text. See Configuring your logon warning message title and text on page 134.

About this task

If you configured a logon warning message, enable the message. Users receive the message when they log on to Contact Center Manager Administration.

If you did not configure a logon warning message, proceed to Configuring Real-Time Reporting on page 136.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. On the **Apps** screen, in the **Avaya** section, select **Manager Administration Configuration**.
3. In the Avaya Applications Configuration window, in the right pane, click the **Change Login Warning Settings** icon.
4. In the **Login Warning Properties** dialog box, select the **Use Login Warning Message** check box.
5. Click **OK**.
6. Close all windows.
7. If the Contact Center Manager Server is part of a networked contact center, configure this setting on each Contact Center Manager Administration server.

Configuring Real-Time Reporting

Before you begin

- Ensure that the IP multicast addresses that you select for Real-time Statistics Multicast (RSM) sending and receiving are in the 224.0.1.0 to 239.255.255.255 range. Check with your network administrator for acceptable IP multicast addresses for your specific network.
- Ensure that the Contact Center Manager Administration server sending and receiving IP multicast addresses differ.
- If the Contact Center Manager Server is part of a networked contact center, ensure that all Contact Center Manager Servers within the network have the same multicast IP address.
- If your solution includes multiple instances of Contact Center Manager Administration, you must configure each Contact Center Manager Administration with different multicast IP send addresses.

Note:

In a High Availability solution, the active CCMA and the standby CCMA must have the same multicast IP send address.

About this task

Configure Real-Time Reporting if you plan to use multicast-based data transmission. You must configure the IP multicast addresses for the Contact Center Manager Server to receive Multicast data and the Contact Center Manager Administration server sending IP multicast data.

If you configure a replicating server, you must select the multicast transmission options under the Real-time Reporting Configuration.

If you plan to use unicast-based transmission, skip this procedure.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. On the **Apps** screen, in the **Avaya** section, select **Manager Administration Configuration**.
3. In the Avaya Applications Configuration window, in the left pane, navigate to **Avaya** > **Applications** > **Real-Time Reporting**.
4. In the right pane, click the **RTR Registry Settings** icon.
5. In the **RTR Properties** dialog box, in the **IP Receive Address** box, type the Contact Center Manager Administration server receiving IP multicast address.
6. In the **IP Send Address** box, type the Contact Center Manager Administration server sending IP multicast address.
7. For the **Output Rate** box and the **Transform Rate** box, accept the default values (5000 and 1000).

   Important:

   You can adjust the default values, however, reducing the Output Rate value and the Transform Rate value increases the workload on the Contact Center Manager Administration server.
8. For the **OAM Timeout** box, accept the default value (120 000).
9. Select the **Compress Realtime Data Packets** check box.

   Important:

   If you clear this check box, you disable real-time data packet compression.
10. In the **Transmission Options** area, select one of the following options:
    - If your network supports multicast traffic, select **Multicast**. Avaya recommends this option.
    - If you want no multicast traffic on your network, select **Unicast**.
    - To support both transmission types, select **Multicast and Unicast**.
11. If you selected the **Multicast** option, proceed to step 14 on page 137.
12. In the **Maximum Unicast Sessions** box, type the maximum number of simultaneous unicast sessions that you want the server to allow.
13. Select the **Restart Real Time Reporting Service** check box.
14. Click **OK**.

    The Restart ICERtdService status window appears while the service is restarts and closes after the service successfully restarts.
15. Close all windows to complete the procedure.

Variable definitions

Name	Description
OAM Timeout	Maximum limit is 5 minutes (300000 milliseconds). Changes to OAM Timeout take effect only after you restart the IceRTDService.
Transmission Options	The transmission of real-time data from the CCMA to the clients. It does not relate to the transmission of real-time data between CCMS and CCMA.
Maximum Unicast Sessions	The maximum number of client-side unicast sessions that you want the CCMA server to allow. It does not relate to the transmission of unicast data between the CCMS and CCMA.

Procedure job aid

You might need to increase the OAM Timeout value if the following situations occur:

- You can see no partition elements in the right pane when you create or view a partition in Access and Partition Management. This can occur when a large amount of information is stored on Contact Center Manager Server and the network is slow.
- Your contact center has a large numbers of agents or skillsets. In this case, it might not be possible to return a large list of agents or skillsets when viewing a report using the Historical Reporting component or running Agent or Skillset real time displays in the Real-Time Reporting component.

Increase the OAM Timeout value to provide more time to collect the partition elements on each server. Avaya recommends that you increase this value in increments of 10 000 (milliseconds).

Configuring Emergency Help

Before you begin

- Ensure that you have administrator privileges on the Contact Center Manager Administration server.
- Ensure that the Emergency Help Configuration settings on the replicating server match the Emergency Help Configuration settings on the primary server. This applies only if you configure a replicating server.

About this task

Configure Emergency Help for an agent. If the Emergency Help feature is configured and an agent requests assistance, the supervisor is notified through the Emergency Help component of Contact Center Manager Administration. For example, if a caller is abusive to an agent, the agent can press Emergency on the phone and the supervisor is notified.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. On the **Apps** screen, in the **Avaya** section, select **Manager Administration Configuration**.
3. In the Avaya Applications Configuration window, in the left pane, navigate to **Avaya** > **Applications** > **Emergency Help**.
4. In the right pane, click the **Emergency Help Registry Settings** icon.
5. In the **EH Properties** dialog box, in the **IP Send Address** box, type the IP address to which the Contact Center Manager Administration server sends Emergency Help information.
6. Select the **Restart Emergency Help Service** check box.
7. Click **OK** to restart Emergency Help.
8. Close all windows to complete the procedure.

Configuring email notifications for Historical reporting

Before you begin

- Check with the Administrator of the email server for setup configuration. If anonymous users are allowed, a user name and password is not required.
- Install an SMTP Server as an operating system component for Contact Center Manager Administration.

About this task

Configure Simple Mail Transfer Protocol (SMTP) to send an email notification to report recipients when the Historical Reporting component of Contact Center Manager Administration generates a scheduled report.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. On the **Apps** screen, in the **Avaya** section, select **Manager Administration Configuration**.
3. Double-click **Email Notification Settings**.
4. Enter the **SMTP Server** name.

   If the Contact Center Manager Administration server is used, for example localhost, then follow the steps under Configuring SMTP Server on the Contact Center Manager Administration Server on page 140.
5. Enter the **SMTP Server Port number**.

6. Enter the **From Address**.
7. If the SMTP Server requires authentication select **Authentication Required**, otherwise skip to step 11 on page 140.
8. For **Username**, enter the email user name.
9. For **Password**, enter the email user password.
10. If the SMTP server requires a secure connection, select **SSL Required**. Contact Center no longer supports Secure Sockets Layer (SSL); using this field enables Transport Layer Security (TLS) for SMTP communication.
11. Click **OK**.

Variable definitions

Name	Description
SMTP Server	The name of the SMTP server. The default is localhost.
Port	The port number of the SMTP server. The default is 25.
From Address	The email address from which notifications are sent.
Authentication Required	Select if the SMTP server requires authentication.
User Name	The email user name.
Password	The email user password.
Enable SSL	Select if the SMTP server requires secure communications. Contact Center no longer supports Secure Sockets Layer (SSL); using this field enables Transport Layer Security (TLS) for SMTP communication.

Configuring SMTP Server on the Contact Center Manager Administration Server

About this task

If you entered the Contact Center Manager Administration Server, for example localhost, as the SMTP Server, then you must configure the SMTP Server on the Contact Center Manager Administration server.

Configure Simple Mail Transfer Protocol (SMTP) to send an email notification to report recipients when the Historical Reporting component of Contact Center Manager Administration generates a scheduled report.

You must install and configure the SMTP server on the Contact Center Manager Administration server.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. On the **Start** screen, click **Administrative Tools** > **Internet Information Services (IIS) 6.0 Manager**.
3. In the left pane of the Internet Information Services (IIS) 6.0 Manager window, expand **<Computer Name> (local computer)**.
4. Right-click the **SMTP Virtual Server #1**, and click **Properties**.
5. In the **Default SMTP Virtual Server Properties** dialog box, click the **Delivery** tab.
6. Click **Advanced**.
7. In the **Fully qualified domain name** box, type the domain name of the Contact Center Manager Administration server.
8. Click **Check DNS** to validate the name of the Domain Name Service (DNS).
9. On the **Confirmation** box, click **OK**.
10. In the **Smart host** box, type the host name of the Microsoft Exchange server.
11. Select the **Attempt direct delivery before sending to smart host** check box.
12. Select the **Perform reverse DNS** lookup on incoming messages check box.
13. Click **OK** to close the Advanced Delivery dialog box.
14. Click the **Access** tab.
15. Click **Authentication**.
16. Clear the **Basic authentication** check box.
17. Select the **Anonymous Access** check box.
18. Click **OK** to close the Authentication dialog box.
19. Click **Connection**.
20. Click **All except the list below**.
21. Click **OK**.
22. Click the **Messages** tab.
23. Select all check boxes.
24. In the **Send copy of Non-Delivery Report** to box, type the email address of the person who monitors the Non-Delivery report.
25. Click **OK** to close the Default SMTP Virtual Server Properties window.

Variable definitions

Name	Description
Computer Name	The name of your local computer.
Fully qualified domain name (FQDN)	The format of the FQDN is <computername>.<domain name>.com Example: pcbox123.softwarehouse.com Domain names can include alphanumeric characters only, including hyphens (-) and periods (.) but not underscores (_).
Smart host	The smart host name must be the name of a valid mail server. Check the properties of your Microsoft exchange server to find the Smart Host name, or contact your System Administrator.

Creating a shared folder to export historical reports

Before you begin

- Grant read permissions to the shared folder on the Contact Center Manager Administration server so that users can copy the exported report files to their desktops.
- Grant each user access rights to the shared folder on the Contact Center Manager Administration server so that users can access the saved reports.
- Grant change and read permissions to the users who can access the scheduled report account; for example, the iceAdmin account or the domain account.

About this task

Create a shared folder to export historical reports if you want multiple users to access scheduled historical reports from the same folder. The reports are exported locally to the shared folder on the Contact Center Manager Administration server.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Create a folder.
3. Right-click the new folder and select **Sharing with** > **Specific people**.
4. In the **File Sharing** dialog box, select **Everyone**, or the **iceAdmin**, or the **domain account** option.
5. Click **Add**.
6. To grant change and read permissions, select **Everyone**, or the **iceAdmin**, or the **domain account** and select the **Read/Write** option from the **Permission Level** drop-down list.

7. Click **Share**.
8. In the **Network Discovery and file sharing** dialog box select **No, make the network that I am connected to a private network**.
9. Click **Done**.

Configuring Contact Center Manager Administration security settings

Before you begin

- Ensure that you have administrator privileges on the Contact Center Manager Administration server.

About this task

For new installations of Contact Center Release 7.0 Feature Pack 1 and later, Contact Center Manager Administration(CCMA) security settings are turned on by default. If you are upgrading from Contact Center Release 7.0, your existing CCMA security settings are not modified. You can customize various security settings that appear when users attempt to log on to the CCMA server using the CCMA Security Settings window.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. On the **Apps** screen, in the **Avaya** section, select **Manager Administration Configuration**.
3. In the Avaya Applications Configuration window, in the right pane, click the **CCMA Security Settings** icon.
4. In the CCMA Security Settings window, configure the following settings:
    a. If you want CCMA to display the date and time of the users last login, select **Show time of last login**.
    b. If you want CCMA to temporarily lock out users if users incorrectly enter the application password a specified number of times, select **Lockout Enabled** and configure the following settings:
        a. Enter the number of times the users can enter an incorrect password in **Failed attempts before lockout**. By default, users can enter an incorrect password three times before getting locked out.
        b. Enter the time, in minutes, for which the users get locked out of CCMA in **Lockout Duration**. By default, the lockout period is three minutes.

c. If you want the password used in CCMA to expire after a specified duration, in the Password expiry section, select **Enabled** and configure the following settings:

   a. Enter the number of days from when CCMA displays a warning to the users about CCMA password expiry in **Expiry warning period**. By default, CCMA displays a warning about password expiry 14 days before the CCMA password expires.

   b. Enter the number of days after which the CCMA password must be changed in **Maximum password age**. By default, the CCMA password must be changed every 30 days.

d. If you want CCMA to force users to change their passwords when users log on to Contact Center Manager Administration for the first time, select **Force password change on first login**.

Installing the Orchestration Designer

About this task

Install the Orchestration Designer to manage Contact Center applications. You can use applications to route contacts based on certain criteria from the contact such as skillset or customer name.

Procedure

1. Log on to the Contact Center Manager Administration browser.
2. On the launchpad, click **Scripting**.
3. In the Scripting window, on the menu, click **Orchestration Designer**, and then click **Launch Orchestration Designer**.
4. In the message box requesting you to download a .msi file, click **OK**.
5. In the dialog box, click **Run**.
6. In the **Orchestration Designer - InstallShield Wizard**, click Next.
7. Accept the terms in the license agreement, and click **Next**.
8. In the **User Name,** type a name.
9. In the **Organization**, type your company name.
10. Select one of the following options:
    - Anyone who uses this computer (all users)
    - Only for me (User Name)
11. Click **Next**.
12. Accept the default Destination Folder.

    OR

Click **Browse** to select a different location.

This is the folder is where the offline application is installed.

13. Click **Next**.
14. Click **Install**.
15. Click **Finish**.

Procedure job aid

Information about the Orchestration Designer is found in *Using Contact Center Orchestration Designer*.

Configuring Agent Desktop Displays parameters on the server

Before you begin

- Configure the Contact Center Manager Administration IP send address in the Real-Time Reporting Configuration tool.

About this task

The Avaya Agent Desktop Display component functions only if you use the multicast communication method from the Contact Center Manager Administration server to the client.

To use Agent Desktop Displays on a client, you must configure the parameters on the Contact Center Manager Administration server. You must also have the Real-Time Reporting component installed and configured on the Contact Center Manager Administration server for Agent Desktop Displays to function properly.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Agent Desktop Displays Configuration**.
2. On the Configuration Parameters window, confirm that the address in the **IP multicast address** box is the Contact Center Manager Administration server IP send address in the Real-Time Reporting Configuration Tool.
3. In the **Refresh rate (seconds)** box, type the rate in seconds at which you want to refresh the display of real-time data.
4. In the **Max agents** box, type the maximum number of agents who can simultaneously log on to the Agent Desktop Displays component and view the real-time statistics.
5. In the **View** mode list, select the **Moving Window** or **Interval-to-date** mode.

6. To require agents to log on to their phones before they can start Agent Desktop Displays, select the **Agents phoneset login required for ADD** check box.
7. To disable automatic notifications for Agent Desktop Displays client upgrades, select the **Disable Automatic ADD Client Upgrade** check box.
8. In the **Statistics Configuration** table, choose the statistics to appear in the Agent Desktop Displays.
9. To add the statistics column to the displays, select the **Show** check box for each statistic you want to add.
10. To arrange the order in which the statistics columns appear, use the column order buttons, select the statistic to move, and then click the up or down button to change the position.
11. To configure the threshold display color, highlight a statistic, and then from the following lists, select the threshold color for that statistic.
12. If you want the selected statistic to blink in the Agent Desktop Displays when the value reaches the threshold, select the **Blink** check box.
13. If you want the Agent Desktop Displays to beep when the value reaches the threshold, select the **Beep** check box. If you do not select the **Beep** check box, proceed to step 15 on page 146.
14. To indicate that a beep occurs only once, select the **Once** option.

    OR

    To indicate that a beep occurs continuously, until the statistic reaches an acceptable value, select **Continuously**.
15. Click **Save**.

Variable definitions

Name	Description
Agent Desktop Displays Agents phoneset login required for	Require agents to log on to their phones before they start ADD. If this check box is clear, when an agent logs on to Agent Desktop Displays, the agent sees data only if other agents log on to skillsets to which that agent is assigned.
IP multicast address	The IP multicast addresses that you select for RSM sending and receiving must be within the 224.0.1.0 and 239.255.255.255 range. Check with your network administrator for acceptable IP multicast addresses for your specific network.

Table continues…

Name	Description
Max agents	The maximum number of agents who can simultaneously log on to the Agent Desktop Displays component and view the real-time statistics. When the number of agents who log on to the application reaches this number, additional agents who try to log on receive a message informing them to try again later. Each connected Agent Desktop Displays client is registered on the server. An inactive Agent Desktop Displays client is unregistered if it is idle for over three minutes. If you leave this box empty, the system uses the default and maximum value of 1000 agents.
Refresh rate (seconds)	The rate in seconds at which you want to refresh the display of real-time data. The minimum value is 2 seconds. If you leave this box empty, the system uses the default value of 5 seconds.
View mode	The method in which you want to view the collected data: • Moving window: In moving window mode, statistics shown represent the last 10 minutes of system activity. • Interval-to-date: In interval-to-date mode, statistics are collected only for the current interval. When the interval ends, data fields reset to 0 and collection begins for the next interval. The interval can correspond to a work shift or to another system-defined period.

Changing the password for the iceAdmin user account

Before you begin

- Ensure that you have administrative privileges on the Contact Center server.
- Obtain the domain account name and password from your administrator to export reports to a domain account.
- Use System Control and Monitor Utility (SCMU) to stop all Contact Center Manager Administration (CCMA) services.
- Reset Internet Information Services (IIS) (using the **`iisreset`** command) on the Contact Center server.

About this task

Follow this procedure to change the iceAdmin user account password in both Windows Server 2012 and CCMA.

For example, if your organization's user account policy requires you to change Windows passwords at a set interval, you will have to change the iceAdmin user account password.

If you forget the iceAdmin password and need to reset it, first reset the iceAdmin Windows user account password to a temporary value using the User Accounts utility in Control Panel. Then follow this procedure to configure a new iceAdmin password, using the temporary value as the Old Password.

Important:

In High Availability solutions, repeat this procedure on the standby server and RGN server.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Manager Administration Configuration**.
2. In the Avaya Applications Configuration window, in the left pane, expand **Avaya** > **Applications** > **IceAdmin Password Change**.
3. In the right pane, click the **IceAdmin Password Change** icon.
4. In the **IceAdmin Password Change** dialog box, In the **Old Password** box, type the old password for this account.
5. In the **New Password** box, type the new password for the iceAdmin user account.
6. In the **Confirm Password** box, type the password again.
7. If you do not want to export scheduled reports to a domain account, or if the **Domain Account** button is unavailable, proceed to step 14 on page 148.
8. To export scheduled reports to a domain account, click **Domain Account**.
9. In the **Optional Domain Account Setup** dialog box, verify that the correct domain is identified or enter the correct domain in the **Domain Name** box.
10. In the **Enter Domain Account** box, type the domain account.
11. In the **Enter Domain Account Password** box, type the domain account password.

    Important:

    You must enter the correct domain account password. If the password is incorrect, the process cannot continue.
12. In the **Confirm Domain Account Password** box, retype the domain account password.
13. Click **OK**.

    The iceAdmin Password Change dialog box reappears and activates all scheduled reports using the domain account instead of the local iceAdmin account.
14. Click **OK**.

15. Use System Control and Monitor Utility (SCMU) to start CCMA.

Configuring the LPR port for printers

Before you begin

- Ensure that you have the Windows Server 2012 Release 2 installation disk.

About this task

Configure the Line Printer Remote (LPR) port on your server to connect a printer.

Procedure

1. Log on to the server.
2. In the **Control Panel**, click **Programs**.
3. Select **Programs and Features**, right-click **Turn Windows features on or off**.

   The Server Manager appears.
4. In the Server Manager window, in the right pane, select **Features**.
5. Click **Add Features**.

   The Add Features Wizard appears.
6. In the Select Features window, select **LPR Port Monitor**.
7. Click **Next**.
8. In the Confirm Installation Selections window, click **Install**.

   The Installation Progress window appears.
9. In the Installation Completion window, click **Close**.

Configuring a network printer for CCMA

Before you begin

- Ensure that you have administrator privileges on the Contact Center Manager Administration (CCMA) server.
- Configure a network printer.
- Know the computer name of the server to which the network printer is attached.
- Know the share name of the printer.
- Ensure that the default CCMA Administration account (iceAdmin) or the alternate domain account has permissions to use the network printer. For more information on specifying an alternate domain account, see Changing the password for the iceAdmin user account on page 147.

- Install the network printer driver on the Contact Center server.

About this task

Configure Contact Center Manager Administration to print on-demand and scheduled historical reports and scripts to a network printer. Because the default CCMA Administration account (iceAdmin) has reduced privileges on Windows Server 2012, you must use a Powershell script to set up the network printer.

Procedure

1. Log on to the Contact Center server with Administrative privileges.
2. Create a new Powershell script file with the following content:

   ```
   $printer = '\\serverName\serverPrinter' $iceAdminPassword = 'icePasswd'
   $taskAction = New-ScheduledTaskAction –Execute 'C:\Windows\System32\cmd.exe' -
   Argument ('/C rundll32 printui.dll,PrintUIEntry /in /n' + $printer) $taskTrigger
   = New-ScheduledTaskTrigger –Once -At
   ([System.DateTime]::Now).Add([System.TimeSpan]::FromMinutes(1)) $taskSetting =
   New-ScheduledTaskSettingsSet Register-ScheduledTask -TaskName 'AddPrinter' -
   Action $taskAction -Trigger $taskTrigger -Settings $taskSetting -User 'iceAdmin' -
   Password $iceAdminPassword
   ```

   where `serverName` is the name of the network print server, `serverPrinter` is the name of the network printer, and `icePasswd` is the password for the iceAdmin user account.
3. Run the Powershell script on the server command line, for example:

   ```
   powershell -file "C:\Users\Administrator\Documents\ConfigureNetworkPrinter.ps1"
   ```

Installing the XML Automated Assignments feature

Before you begin

- Ensure that you have administrator privileges on the Contact Center Manager Administration server.

About this task

Use the XML Automated Assignments feature to simultaneously update multiple supervisor and skillset assignments by creating a specially formatted Extensible Markup Language (XML) file.

This is an optional feature that you use with the Contact Center Manager Server component.

For information about obtaining the XML Automated Assignment toolkit, contact a member of the Developer Program at www.avaya.com/developer. General information about the Developer Program, including an online membership application, is also available on this site.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Insert the Contact Center Installation DVD into the drive.
3. On the DVD, browse to **Installed Software** > **CCMA** > **XMLAutomatedAssignments**.

4. Expand the **XMLAutomatedAssignments** folder.
5. In this folder, double-click **CCMAXMLAutomatedAssignmentsService.msi**.
6. In the **Welcome to the InstallShield Wizard for CCMA XML Automated Assignments Service** dialog box, click **Next**.
7. In the **Destination Folder** dialog box, click **Change** to select the folder in which to store the XML files to be parsed, and the folder in which the system stores XML files that it cannot parse due to errors. You can also accept the default folders.
8. Click **Next**.
9. In the **Ready to Install the Program** dialog box, click **Install**.
10. In the **Completed** dialog box, click **Finish**.

Configuring Avaya Call Recording and Quality Monitoring

About this task

You can use Call Recording and Quality Monitoring (CRQM) to navigate to the management applications for the CRQM system.

To define server names and URLs, use the Configuration component in the Contact Center Manager Administration client. Contact Center Manager Administration users can then use the server names and URLs to start the CRQM applications.

Procedure

1. Log on to the Contact Center Manager Administration browser.
2. On the launchpad, click **Configuration**.
3. In the left pane, select the Contact Center Manager Server on which to configure CRQM.
4. Expand the list and select **Call Recording and Quality Monitoring**.
5. In the **Primary Server Name** box, type the name of the primary call recording server.
6. In the **Primary Server URL** box, type the URL for the Call Recording manager software which runs on the Call Recording server.
7. In the **Standby Server Name** box, type the name of the standby call recording server.
8. In the **Standby Server URL** box, type the URL for the standby Call Recording manager software which runs on the standby Call Recording server.
9. In the **Slave Servers** section, enter the name and URL of each slave Call Recording server.
10. Click the **Quality Monitoring** heading.
11. In the **Quality Monitoring Server Name** box, type the name of the Quality Monitoring server.

12. In the **Quality Monitoring Server URL**, type the URL for the Quality Monitoring manager software which runs on the Quality Monitoring server.
13. Click the **Quality Viewer** heading.
14. In the **Quality Viewer Server Name** box, type the name of the Quality Viewer server.
15. In the **Quality Viewer Server URL** box, type the URL for the Quality Viewer manager software that runs on the Quality Viewer server.
16. Click the **Quality Archiver** heading.
17. In the **Quality Archiver Server Name** box, type the name of the Quality Archiver server.
18. In the **Quality Archiver Server URL** box, type the URL for the Quality Archiver software that runs on the Quality Archiver server.
19. Click **Submit** to save the changes.

Configuring CDN Landing Pads for Universal Networking or Integrated Reporting

Before you begin

Configure the CDNs on the telephony PABX. For information about configuring a CDN on the telephony PABX, see *Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration*.

About this task

A Landing Pad associates data with a call that is sent to a target site. For Universal Networking the target site reserves a Landing Pad for the call ID at the source site. The source site then requests the call server to send the call to the Landing Pad. For Integrated Reporting, only one site is involved. When the call arrives on the Landing Pad at the target site, the Contact Center Manager Server maps the call to the original call ID, along with other data specified in the Landing Pad, to determine how to route the call. For Universal Networking, the call is routed to an agent. For Integrated Reporting, the call is routed to a CDN specified in the Landing Pad data by the application that originated the call. Landing Pads can be configured to use either CDNs or DNISs.

For each site configured to use Universal Networking or Integrated Reporting, you must define the Landing Pads. If the site can use CDN Landing Pads, you must configure CDN Landing Pads. If the site can use DNIS Landing Pads, you must configure DNIS Landing Pads and the DNIS Network CDN. Integrated Reporting is supported only when CDN Landing Pads are used.

CDN Landing Pads can also be used to assign a call ID to an incoming call for the purpose of Integrated Reporting, and to attach data to the call without requiring CTI.

Procedure

1. Log on to Contact Center Manager Administration.
2. Click **Configuration**.

3. On the system tree, in the Configuration component, double-click the server in Contact Center Manager Server to which you want to add the Landing Pad CDN (Route Point).
4. Click the **CDNs (Route Points)** heading.
5. Select the **Landing Pads** tab.
6. In the empty **Name** box at the bottom of the table, type the name of the new Landing Pad CDN (Route Point).
7. Press **Tab**.
8. In the **Number** box, type the Landing Pad CDN (Route Point) number. This number must match the number configured on the telephony PABX.
9. For SIP-enabled contact centers, you must configure the Landing Pad URI. This field is only present for SIP-enabled contact centers. In the **URI** box, type the value for the Universal Resource Indicator (URI) of the CDN (Route Point) on the SIP server.
10. Select the **Acquired?** check box to acquire the CDN.
11. Press **Tab** to submit your changes.

Configuring a DNIS Landing Pad for Universal Networking

Before you begin

Configure the DNISs on the telephony PABX. For information about configuring the telephony PABX, see *Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration*.

About this task

A Landing Pad associates data with a call that is sent to a target site. For Universal Networking the target site reserves a Landing Pad for the call ID at the source site. The source site then requests the call server to send the call to the Landing Pad. When the call arrives on the Landing Pad at the target site, the Contact Center Manager Server maps the call to the original call ID, along with other data specified in the Landing Pad, to determine how to route the call. For Universal Networking, the call is routed to an agent.

For each site configured to use Universal Networking, you must define the Landing Pads. If the site can use DNIS Landing Pads, you must configure DNIS Landing Pads and the DNIS Network CDN.

Integrated Reporting is not supported when DNIS Landing Pads are used.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the launchpad, click **Configuration**.
3. In the left pane, expand the server under which to add the DNIS Landing Pad.
4. Click the **DNIS** heading.

5. Select the **Landing Pads** tab.
6. In **Name** box, type the name of the new DNIS.
7. In the **Number** box, type the DNIS number. This number must match the number configured on the telephony PABX.
8. Optionally, in the **Description** box, type a description for the DNIS Landing Pad.
9. Press **Tab** to save your changes.

Chapter 17: Avaya Communication Server 1000 Data Extraction Tool operation

The Avaya Communication Server 1000 Data Extraction Tool is an application that extracts information about resources such as Terminal Numbers (TNs), voice ports, Controlled Directory Numbers (CDNs), Interactive Voice Response Automatic Call Distribution DNs (IVR ACD-DNs), and routes from an Avaya Communication Server 1000 PABX. The tool saves this information in Excel spreadsheets.

To save data entry time, you can use Excel spreadsheets with the Contact Center Manager Administration Configuration upload utility by copying the Avaya Communication Server 1000 PABX data and pasting it into the Configuration Tool spreadsheet templates that you download from the Contact Center Manager Administration application.

You cannot upload data from the Avaya Communication Server 1000 Data Extraction Tool spreadsheets directly to Contact Center Manager Administration. You must copy the data from the Avaya Communication Server 1000 Data Extraction Tool spreadsheet into the Contact Center Manager Administration Configuration Tool spreadsheet and then upload the data. Contact Center Manager Administration does not support uploading directly from the Avaya Communication Server 1000 Data Extraction Tool spreadsheets.

For more information about Contact Center Manager Administration Configuration Tool spreadsheets, see the Contact Center Manager Administration online Help.

Prerequisites to Avaya Communication Server 1000 Data Extraction Tool

Procedure

Connect to Avaya Communication Server 1000.

Extracting data from a serial connection

Before you begin

- Ensure your serial connection parameters match the parameters of the Avaya Communication Server 1000. Contact your telephony PABX administrator if you do not know which parameters to select.

About this task

Extract data from the Avaya Communication Server 1000 through a serial connection using an available serial port on your computer.

When you install and use the Avaya Communication Server 1000 Data Extraction Tool on the client PC, the tool connects directly to the Avaya Communication Server 1000 through the serial port; it does not connect to the telephony PABX through a server.

Procedure

1. On the **Desktop** screen, click **Contact Center** > **CS1000 Data Extraction Tool** > **CS1000 Data Extraction Tool**.
2. In the **Select Options** dialog box, select **Serial Port**, and then click **Next**.
3. In the **CS 1000 Data Extraction Tool - Step 1 of 4** dialog box, from the **Connect Using** list, select your available COM port to configure your serial connection parameters
4. In the **Connection Preferences** area, select your connection preferences.
5. In the **Flow Control** area, select a flow control option.
6. To test your COM port, click **Test**.

   A message appears in the Status box informing you if your COM port is working.
7. Click **Next**.
8. In the **CS 1000 Data Extraction Tool - Step 2 of 4** dialog box, in the **Switch Resources** area, select the resources to download from the telephony PABX.
9. In the **Login Account** section, enter your user ID and password for the telephony PABX.

   The default user ID is admin.

   Important:

   Do not type Avaya Communication Server 1000 overlay commands in the User ID box. Type only your user ID for the Avaya Communication Server 1000 telephony PABX.
10. In the **Select option to load TN Data** section, select the overlay to use to download TN data:
    - LD 20 All TNS
    - LD 81 Agent & Supervisors TNS
11. In the **Customer Number** box, type your customer number.
12. Click **Browse** to select the location in which to save exported data.

13. In the **Save As** dialog box, click **OK**.

    The path you select appears in the File name box.

14. Click **Next**.

    The CS 1000 Data Extraction Tool - Step 3 of 4 window appears, confirming your selected resources, user ID, and exported file name.

15. If the **Failed to logon** dialog box appears, exit the Avaya Communication Server 1000 Data Extraction Tool, confirm your settings, restart the Avaya Communication Server 1000 Data Extraction Tool, and then attempt to log on again.

16. Click **Next** to download the data.

    The CS 1000 Data Extraction Tool - Step 4 of 4 window appears indicating the progress of connecting to the Avaya Communication Server 1000, retrieving the data, and exporting it to the Excel file.

17. Click **Finish** when the data extraction is complete.

Extracting data using a modem

Before you begin

- Connect the Avaya Communication Server 1000 PABX to a modem.

About this task

Extract data by using a modem to connect to the Avaya Communication Server 1000.

Procedure

1. On the **Desktop** screen, click **Contact Center** > **CS1000 Data Extraction Tool** > **CS1000 Data Extraction Tool**.
2. In the **Select Options** dialog box, select **Modem**.
3. Click **Next**.
4. In the **CS 1000 Data Extraction Tool - Step 1 of 4** dialog box, from the **Connect using** list, select the modem to use.
5. In the **Phone number** box, type the phone number used for the modem at the Avaya Communication Server 1000 telephony PABX.
6. To test your COM port, click **Test**.

   A message appears in the Status box informing you if your COM port is working.

7. Click **Next**.
8. In the **CS 1000 Data Extraction Tool - Step 2 of 4** dialog box, in the **Switch Resources** section, select the resources to download from the telephony PABX.

9. In the **Login Account** section, type your user ID and password for the telephony PABX.
10. In the **Select option to load TN Data** section, select which overlay to use to download TN data:
    - LD 20 All TNS
    - LD 81 Agent & Supervisors TNS
11. In the **Customer Number** box, type your customer number.
12. Click **Browse** to select the location to save exported data.

    The Browse for Folder window appears with the default folder selected.
13. Accept the default selection, or navigate to the folder of your choice.
14. Click **OK**.

    The path you select appears in the File name box.
15. Click **Next**.

    The CS 1000 Data Extraction Tool - Step 3 of 4 dialog box appears, confirming your selected resources, user ID, and exported file name.
16. Click **Next** to download the data.

    The CS 1000 Data Extraction Tool - Step 4 of 4 dialog box appears indicating the progress of connecting to the Avaya Communication Server 1000, retrieving the data, and exporting it to the Excel file.
17. Click **Finish** when the data extraction is complete.

Extracting data from a file

Before you begin

- Ensure that you have at least one file from which to extract data.

About this task

You can use the Extract from File option to extract data from an output file that you captured from the Avaya Communication Server 1000 and saved on your computer.

Procedure

1. On the **Desktop** screen, click **Contact Center** > **CS1000 Data Extraction Tool** > **CS1000 Data Extraction Tool**.
2. In the **Select Options** dialog box, select **File**.
3. Click **Next**.
4. In the **CS 1000 Data Extraction Tool - Step 1 of 4** dialog box, in the **Source File name** box, type the name of the file that contains the Avaya Communication Server 1000 data.

OR

Click **Browse** to navigate to the file.

5. Click **Next**.
6. In the **CS 1000 Data Extraction Tool - Step 2 of 4** dialog box, in the **Switch Resources** section, check the telephony PABX resources to download from the file.
7. In the **File name** box, type the path and file name.

   OR

   Click **Browse** to select the location in which to save exported data.

   The Browse for Folder dialog box appears with the default folder selected.
8. Click **OK**.
9. Click **Next**.

   The CS 1000 Data Extraction Tool - Step 3 of 4 dialog box appears, confirming your selected resources and the exported file name.
10. Click **Next**.

    The CS 1000 Data Extraction Tool - Step 4 of 4 dialog box appears indicating the progress of connecting to the output file and exporting the data you selected to the Excel file.
11. Click **Finish** when the data extraction is complete.

Capturing Terminal Number data

Before you begin

- Connect to Overlay program 20.

About this task

Capture a list of all configured Terminal Numbers (TNs).

Procedure

1. At the **LD** prompt, enter

   ```
   20
   ```
2. At the **REG** prompt, enter

   ```
   PRT
   ```
3. At the **TYPE** prompt, enter

   ```
   TNB
   ```
4. AT the **TN** prompt, enter

TN

5. At the **CDEN** prompt, enter

   CDEN

6. At the **CUST** prompt, enter the customer number.
7. At the **DATE** prompt, enter the date from which to print.
8. At the **PAGE** prompt, enter `Yes` to print data for each page.
9. At the **DES** prompt, enter a designator.

Example of capturing terminal data

About this task

An example of the output follows:

```
DES LAB30
TN 002 0 00 00
TYPE 500
CDEN 4D
CUST 0
WRLS NO
DN 7050 0 MARP
CPND
NAME 500 set-1
XPLN 9
DISPLAY_FMT FIRST,LAST
AST NO
IAPG 0
HUNT
TGAR 0
LDN NO
NCOS 0
SGRP 0 RNPG 0
XLST
SCI 0
CLS UNR DTN FBD XFA WTA THFD FND HTD ONS
LPR XRA CWD SWD MWD RMMD SMWD LPD XHD CCSD LND TVD
CFTD SFD MRD C6D CNID CLBD AUTU
ICDD CDMD LLCN EHTD MCTD
GPUD DPUD CFXD ARHD OVDD AGTA CLTD LDTD ASCD
MBXD CPFA CPTA DDGA NAMA
MCRD
EXR0 SHL ABDD CFHD DNDY DNO3
CWND USMD USRD BNRD OCBD RTDD RBDD RBHD FAXD
 CNUD CNAD
PGND FTTU
PLEV 02
SPID NONE
PRI 01
AACD NO
AACS NO
MLWU_LANG 0
FTR CFW 16 FTR PHD
FTR ACD 3500 3204
```

```
AGN
DATE 8 MAR 1999
```

Capturing voice port data

Before you begin

- Log on to Overlay program 81.

About this task

You can capture a list of all voice ports configured as TNs on the telephony PABX by using Overlay program 81. To separate voice ports from the other TNs, request only those TNs with the Voice Messaging Allowed (VMA) feature.

Procedure

1. At the **LD** prompt, enter

   `81`

2. At the **REQ** prompt, enter

   `1st`

3. At the **CUST** prompt, enter the customer number.
4. At the **DATE** prompt, enter the date.
5. At the **PAGE** prompt, enter `YES` to print data for each page.
6. At the **DES** prompt, enter the description.
7. At the **FEAT** prompt, enter

   `VMA`

Output example

About this task

VMA	00	TN	010 0 00 01	SL1	MMAIL	NO DATE
VMA	00	TN	010 0 00 08	SL1	MMAIL	15 MAY 1997

Capturing CDN data

Before you begin

- Connect to Overlay 23.

About this task

You can capture a list of all of the CDNs by using Overlay program 23.

Procedure

1. At the **LD** prompt, enter

   ```
   23
   ```

2. At the **REQ** prompt, enter

   ```
   PRT
   ```

3. At the **TYPE** prompt, enter

   ```
   CDN
   ```

4. At the **CUST** prompt, enter the customer number.
5. At the **CDN** prompt, enter

   ```
   CDN
   ```

Example of Overlay 23 output

About this task

```
TYPE CDN
CUST 0
CDN 4911
FRRT
SRRT
....
ACNT
```

Capturing IVR ACD-DN data

Before you begin

- Connect to Overlay 23.

About this task

Capture a list of all of the IVR ACD-DNs by using Overlay program 23.

Procedure

1. At the **LD** prompt, enter

   ```
   23
   ```

2. At the **REQ** prompt, enter

   ```
   prt
   ```

3. At the **TYPE** prompt, enter

   ```
   ACD
   ```

4. At the **CUST** prompt, enter the customer number.
5. At the **ACDN** prompt, enter the ACDN.

Example of output from option 11C for IVR ACD-DNs

About this task

```
TYPE ACD
CUST 0
ACDN 6700
....
CWNT NONE
```

Capturing route data

Before you begin

- Connect to Overlay program 21.

About this task

Capture a list of all of the route numbers from the PABX by using Overlay program 21.

Procedure

1. At the **LD** prompt, enter

   ```
   21
   ```

2. At the **REQ** prompt, enter

   ```
   prt
   ```

3. At the **TYPE** prompt, enter

   ```
   rdb
   ```

4. A the **CUST** prompt, enter the customer number.
5. At the **ROUT** prompt, enter the route.
6. At the **ACOD** prompt, enter the ACOD.

Chapter 18: Language support fundamentals

This chapter provides background information for Language support. If you want to use English across all platforms, you can ignore this chapter.

Contact Center Multimedia (CCMM) and Contact Center Manager Administration (CCMA) support the following languages:

- English
- French (FR)
- German (DE)
- Japanese (JA)
- Russian (RU)
- Simplified Chinese (Zh-CN)
- Traditional Chinese (Zh-TW)
- LA Spanish (ES)
- Brazilian Portuguese (PT-BR)
- Italian (IT)
- Korean (KO)

The following table lists the compatibility between the CCMA language and the Operating System (OS) language family. You can enable only compatible languages on the Contact Center server.

OS language	FR	DE	ES	PT-BR	IT	Zh-CN	Zh-TW	JA	RU	KO
English	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
Any 1 Latin language	Yes	Yes	Yes	Yes	Yes	No	No	No	No	No
Simplified Chinese	No	No	No	No	No	Yes	No	No	No	No
Traditional Chinese	No	No	No	No	No	No	Yes	No	No	No

Table continues…

OS language	FR	DE	ES	PT-BR	IT	Zh-CN	Zh-TW	JA	RU	KO
Japanese	No	No	No	No	No	No	No	Yes	No	No
Russian	No	No	No	No	No	No	No	No	Yes	No
Korean	No	No	No	No	No	No	No	No	No	Yes

You use the Contact Center Manager Administration Language Settings utility to enable additional languages. Access the Language Settings utility from the CCMA Configuration screen. The English language is always enabled and you cannot disable it. The Language Settings utility displays the current server code page for the Contact Center server.

A code page is an internal table that the operating system uses to map symbols (letters, numerals, and punctuation characters) to a number. Different code pages provide support for the character sets used in different languages. Code pages have a number for reference; for example, code page 932 represents the Japanese character set, and code page 950 represents one of the Chinese character sets. In a Contact Center solution, on an English Contact Center server, the Server Code Page is 1252. On a Contact Center server with Japanese, the Server Code Page is 932.

Install the most recent Service Pack and patches to enable the localized languages in the CCMA Language Settings utility. A Service Pack contains all supported languages. For CCMA, you can enable only languages that are appropriate to the local operating system of the server. For example, you can enable the simplified Chinese language on a simplified Chinese OS, but you cannot enable German on a simplified Chinese OS. The client computers operating systems must be of the same language family as the associated server. You can enable multiple languages from the same language family on a single server.

If you enable a language in the Language Settings utility, users see the localized CCMA screens in the preferred language that is set in their client browser. For example, if you enable Spanish in the Language Settings utility, and if Spanish is the preferred language in Internet Explorer on the CCMA client computer, then CCMA appears in Spanish in the CCMA client browser.

For some languages, translations can be different from the terms usually used in your region:

- French: The translation attempts to find terms that are acceptable to both Canadian and European French speakers.
- Latin American (LA) Spanish: The translation attempts to find terms that are acceptable to both Latin American and European Spanish speakers.

Read the Contact Center Service Pack Release Notes for further information. The Service Pack Release Notes contain the most recent information about language support.

Note:

All nodes in a Contact Center Networking deployment, including the Network Control Center server, must be installed on operating systems from the same language family. Contact Center does not support displaying names from two different languages families. For example, a single Contact Center Manager Administration does not support one node with a French operating system and another node with a Russian operating system.

Note:

If the server code page changes, you can still change previously enabled languages. You must disable the languages that are not supported.

Language levels

Contact Center Multimedia and Contact Center Manager Administration support two levels of language environment:

- international environment
- international and local environment

International environment

In the international environment, the graphical user interface, the online Help, and all reports are in English. However, you can enter user information that contains non-ASCII characters (such as agent and supervisor names). Also, you can manage date and time formats from a different regional time zone.

International and local environment

In the combined international and local environment, the graphical user interface, the online Help, and many reports are translated into one of the following supported languages: French, German, Japanese, Italian, Korean, Russian, Simplified Chinese, Traditional Chinese, LA Spanish, and Brazilian Portuguese. Also, you can enter user information that contains non-ASCII characters and you can use date and time formats from a different regional time zone. For details of the reports that are translated for a particular language, see the Contact Center Service Pack Release Notes.

In this environment, you must install the most recent Service Pack on the Contact Center servers. See the Service Pack Release Notes for further information.

Language family compatibility

For Contact Center Manager Administration to function properly, the language family of the operating systems must be compatible across all platforms in the network. If the language versions of the operating systems on the Contact Center Manager Server, Contact Center Multimedia, Contact Center Manager Administration server, and the client PC belong to the same language family, the platforms can coexist on the same network. This compatibility is useful if your contact center supports multiple languages.

The character sets for English are included in all language families. Contact Center Multimedia and Contact Center Manager Administration recognize the following language families:

- Latin-1
- Japanese

- Russian
- Simplified Chinese
- Traditional Chinese
- Korean

Latin-1 includes all Western European languages that use the Latin-1 character set. French, German, Italian, LA Spanish, and Brazilian Portuguese belong to the Latin-1 language family. Agents in the contact center can view Contact Center Manager Administration and Contact Center Multimedia in English, French, German, LA Spanish, Italian, or Brazilian Portuguese. For Latin-1 language family and server compatibility, see the Contact Center Localization Release Notes for further information.

If you use the Japanese language family, users in the same contact center can view Contact Center Manager Administration and Contact Center Multimedia in English or Japanese. If you use the Traditional Chinese language family, users in the same contact center can view Contact Center Manager Administration and Contact Center Multimedia in English or Traditional Chinese. If you use the Simplified Chinese language family, users in the same contact center can view Contact Center Manager Administration and Contact Center Multimedia in English or Simplified Chinese. If you use the Russian language family, users in the same contact center can view Contact Center Manager Administration and Contact Center Multimedia in English or Russian.

Configuring the operating system language

About this task

Perform the following procedure to configure a new language for the Contact Center server operating system. You must perform this procedure to ensure that Contact Center operates correctly when using a new operating system language.

Before you begin

- Download and install the language pack for the language you want to configure on the operating system. Refer to Microsoft documentation for information about language packs.

Procedure

1. Log on to the Contact Center server.
2. On the **Start** screen, click **Control Panel**.
3. In the Control Panel, click **Clock, Language, and Region**.
4. Click **Language**.
5. Click **Add a language**.
6. From the list of languages, select a language and click **Open**.
7. If required, from the list of regional variants, select the regional variant of the language and click **Add**.

8. On the Language window, select the newly added language and click **Move up**.
9. Click **Advanced settings**.
10. Under **Override for Windows display language**, from the drop-down list, select the newly added language.
11. Under **Override for default input method**, from the drop-down list, select the newly added language.
12. Click **Save**.
13. On the **Change display language** dialog box, click **Log off later**.
14. On the Language window, in the left pane, click **Change date, time, or number formats**.
15. On the Region window, select the **Administrative** tab.
16. Click **Copy settings**.
17. On the Welcome screen and new user accounts settings window, select the **Welcome screen and system accounts** check box and the **New user accounts** check box.
18. Click **OK**.
19. Restart the Contact Center server.

Setting the system locale

About this task

Ensure that the Contact Center server system locale matches the operating system language. If the system locale does not match the operating system language, you cannot enable a localized language in Contact Center Manager Administration (CCMA).

Procedure

1. Log on to the Contact Center server.
2. On the **Start** screen, click **Control Panel**.
3. In the Control Panel, click **Clock, Language, and Region**.
4. On the Clock, Language, and Region window, click **Region**.
5. On the Region window, select the **Administrative** tab.
6. Click **Change system locale**.
7. On the Region Settings window, in the **Current system locale** field, select a locale that matches the operating system language.
8. Click **OK**.
9. On the Region window, click **OK**.

Enabling a localized language

Before you begin

- Check that the system locale matches the operating system language setting. For information about setting the system locale, see Setting the system locale on page 168.
- Read the Contact Center Service Pack Release Notes for more information. The Release Notes contain the most recent information about language support.
- Ensure that Contact Center is working before installing the Service Pack.
- Using the Release Pack Installer (RPI) and Avaya Contact Center Update Manager, apply the most recent Service Pack and patches.

About this task

Enable a language using the Contact Center Manager Administration (CCMA) Language Settings utility so that CCMA administrators and users see the localized CCMA screens in their client browsers.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Manager Administration Configuration**.
3. In the Avaya Applications Configuration window, in the right pane, click **Language Settings**.
4. In the Language Settings window, select the required CCMA localized language from the list, and select **Enabled** for that language.
5. Click **Save**.

Accessing the CCMA Web client using a localized language

Before you begin

- Install the most recent Service Pack on the Contact Center server, and enable the required language.

About this task

Access the Contact Center Manager Administration (CCMA) Web client from a Web Browser on an English OS client computer using a localized language. For example, access the CCMA Web client from a Web Browser on an English OS client computer, but using the French language and screens with CCMA. This enables French speaking CCMA administrators and users with an English OS client computer to access and use CCMA with a French language user interface.

If French is enabled in the Language Settings utility, and if French is the preferred language in Internet Explorer on the CCMA client computer, then CCMA appears in French in the CCMA client Internet Explorer browser display.

Procedure

1. From an English client computer, start Internet Explorer.
2. In Internet Explorer, click **Tools** > **Internet Options**.
3. Click **Languages**.
4. Click **Add**.
5. From the list of languages, click the appropriate language. For example, select **French (France) [fr-FR]**.
6. Click **OK**.
7. On the Language Preferences window, use the **Move up** button to move the language you want to use to the top of the **Languages** list.
8. Click **OK** to close the Language Preferences window.
9. Click **OK** to close the Internet Options window.
10. In the **Address** box, type the URL of the server. For example, type `https://<server name>`, OR if you turned off Contact Center security, type `http://<server name>`, where <*server name*> is the computer name of the Contact Center server.

    Important:

    You must log on using the Contact Center server name. Do not use the server IP address.

    The CCMA screens display in French.

Part 5: Network Control Center Server

- Network Control Center server administration on page 172

Chapter 19: Network Control Center server administration

Configure the Network Control Center server to enable skillset routing in your Avaya Aura® Contact Center. Network Skill-Based Routing (NSBR) is an optional feature offered with Contact Center Manager. You can use this feature to route voice contacts to various sites on a network.

Agents and skillsets are configured on a Network Control Center (NCC) and propagated to all servers in the network. If a server has a local skillset with the same name as a network skillset, the network skillset replaces the local skillset. For example, the BestAir Toronto server has a skillset named Sales. When the NCC administrator creates a network skillset named Sales, the Sales skillset at BestAir Toronto becomes a network skillset.

Prerequisites

Procedure

Commission each Contact Center Manager Server in your contact center. See *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.

Adding a site to the NCC

Before you begin

- Log on to the Network Control Center server as Administrator.
- Know the CLAN IP address for each server to add.

Important:

Each server must have a unique CLAN IP address.

About this task

Add a site using the Contact Center Manager Server Network Configuration utility.

You can also use the Network Configuration utility to verify the configuration of the communications database at each server and ensure that each site has valid IP addresses.

Procedure

1. On the **Desktop** screen, click **Start** > **Run**.
2. In the **Run** text box, type `nbconfig -admin`.
3. Click **OK**.
4. In the **Nbconfig** dialog box, click the **Site Table** tab.

   Important:

   Do not select the **Force Synchronization** check box. When you force synchronization, you force each site in the network to request address table information from every other site in the network. This can result in unnecessary use of network bandwidth. (Normally, servers request address table updates only when the NCC notifies them that the site list changed.) Use the **Force Synchronization** option if information at a site is not updated.
5. Click **Add**.
6. In the **Add Site** dialog box, in the **CLAN IP Address** box, type the CLAN IP address of the server.
7. Click **OK**.

   The server is added to the list in the site table.
8. Repeat step 5 on page 173 to step 7 on page 173 for each server in your network.
9. Click **Verify**.

   This verifies the connection to the nodal servers.
10. If all the site names are correct, click **Apply** to update the database and synchronize the site table.

    The **Flags** column shows the progress of synchronization.
11. Click **Refresh** to update the status of the flags.

    Synchronization is complete when an **N** appears in the **Flags** column beside the NCC, and an **S** appears beside each server.
12. Click the **Address Table** tab.

    The communication addresses of the new servers appear on the Address Table page.
13. Click the **OK** button on the Nbconfig window.

Procedure job aid

The **Flags** column in the site table can contain the following values:

Flag	Description
N	Network Control Center (NCC)
S	Server
T	NCC is transferring information to the server
G	NCC is getting information from the server
D	Deleting site
C	Changing site information

Deleting a site from the NCC

Before you begin

Log on to the Network Control Center server as Administrator.

About this task

Delete a site from the NCC using Contact Center Manager Administration and the Contact Center Manager Server Network Configuration utility.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the launchpad, click **Configuration**.
3. On the system tree in the **Configuration** component, double-click the Network Control Center (NCC) server.
4. Select the **Sites** folder.
5. Under **Network Sites**, select the site you want to delete and click **Delete Site**.

   Note:

   You must remove all routing table references before you can delete a site from the NCC.
6. Click **Yes**.
7. On the NCC server, on the **Desktop** screen, click **Start** > **Run**.
8. In the **Run** text box, type `nbconfig -admin`.
9. In the **Nbconfig** dialog box, click the **Site Table** tab.
10. On the **Site Table** tab, select the site to delete and click **Remove**.
11. On the **nbconfig** dialog box, click **Yes**.

Adding access classes

About this task

When you log on to the Contact Center Manager Administration client, you can use the Access and Partition Management component to configure access classes for the Contact Center Manager Servers, and for the Network Control Center (NCC) server.

Procedure

1. Log on to the Contact Center Manager Administration client.
2. On the launchpad, click **Access and Partition Management**.
3. From the **Add** menu, select **New Access Class**.
4. In the **New Access Class Name** box, type a name for the access class.

   Use a descriptive name for the type of user to have this access level or, the type of privileges available at this access level. You can use alphanumeric characters only for the access class name.
5. Click **Submit**.
6. Select a server on which to configure the access class.
7. For each element in the **Access Class Properties** list, select an access level.
8. Click **Submit**.

Adding a site in Contact Center Manager Administration

Before you begin

- Ensure that each site is correctly configured before you add the next site.
- Ensure that CCMS services are running.
- The sites that you can add in this window are those that you configured using the Nbconfig utility when you configure the communications database on the NCC. To add a site that is not listed, you must first add it to the site table using this utility.
- You can add up to 30 sites.

About this task

A site is a location in the network with a telephony PABX and a Contact Center server in CCMS. You must configure the NCC with information about each site in the network so that it can communicate with the network servers and enable the servers to communicate with each other.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the launchpad, click **Configuration**.

3. In the left pane, expand the Network Control Center (NCC) server.
4. Select the **Sites** folder.

   The CDN Landing Pad and DNIS Landing Pad columns appear only if Universal Networking is enabled on the NCC and for at least one site. If Universal Networking is not enabled for a site, the CDN Landing Pad and DNIS Landing Pad check boxes are not selectable.
5. Click **Add Site**.
6. Type the name of the site to add exactly as it appears in the Nbconfig utility.
7. Click **OK**.

   The site name appears in the Site Name box. Wait (at least 5 minutes) for confirmation that the site is up.
8. Click **Refresh Status**.

   The CDN (Route Point) Landing Pad check box, DNIS Landing Pad check box, and Target Node Count box are not selectable when you add the site for the first time.
9. Click **Refresh Status** to modify these boxes.
10. In the **Contact Person** box, type the name of the person to contact if problems with the site occur.
11. In the **Contact Number** box, type the phone number where the contact person at the site can be reached.
12. In the **Comment** box, type additional information about the contact person.
13. In the **Filter Timer** box, type the amount of time to filter the site from the routing tables if it cannot be reached.
14. From the **Relative to GMT** list, select the time difference (in hours) between GMT and the time zone for the site. This information is used for time zone conversion and consolidated reports.
15. To use CDN (Route Point) Landing Pads (for Universal Networking) for this site, select the **CDN (Route Point) Landing Pad** check box.

    This check box is available only if Universal Networking is enabled. If Universal Networking is enabled, you can add a CDN (Route Point) Landing Pad or a DNIS Landing Pad. For more information on configuring Landing Pads, see Configuring Landing Pads for Universal Networking on page 177.
16. To use DNIS Landing Pads (for Universal Networking) for this site, select the **DNIS Landing Pad** check box.

    This check box is available only if Universal Networking is enabled. If Universal Networking is enabled, you can add a CDN (Route Point) Landing Pad or a DNIS Landing Pad. For more information on configuring Landing Pads, see Configuring Landing Pads for Universal Networking on page 177.

17. In the **Target Node Count** box, type the number of target nodes to which the source node sends a Network Agent Request (NAR). You can type digits from 3 to 20.
18. Click another row of the table to submit the site information.

Configuring Landing Pads for Universal Networking

Before you begin

Configure the CDNs and DNIS Network CDNs on the telephony PABX. For information about configuring a CDN on the telephony PABX, see *Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration*.

About this task

Configure CDN or DNIS Landing Pads if Universal Networking is enabled on the NCC server. A Landing Pad identifies the call that is sent to a target site. The target site reserves a Landing Pad for the call ID at the source site. The source site then requests the PABX to send the call to the Landing Pad. When the call arrives on the Landing Pad at the target site, the Contact Center Manager Server maps the call to the original call ID at the source to determine to which agent to present the call.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the launchpad, click **Configuration**.
3. Select a CCMS server on which to configure the Landing Pads.
4. To configure a CDN Landing Pad, in the left pane, click the **CDNs (Route Points)** folder.
5. Select the **Landing Pads** tab.
6. In the **Name** box, type a name for the CDN (Route Point) Landing Pad.
7. In the **Number** box, type the number for the CDN (Route Point) Landing Pad. This number must match the number configured on the PABX.
8. Click any other row in the grid to add the CDN (Route Point) Landing Pad.

   Not Acquired appears in the Status column.
9. For SIP Contact Centers, you must configure the Landing Pad URI. This field is only present for SIP Contact Centers. In the URI box, type the value for the Universal Resource Indicator (URI) of the CDN (Route Point) on the SIP server.
10. Select the **Acquired?** check box for the CDN (Route Point) Landing Pad.
11. Click any other row of the table to acquire the CDN (Route Point) Landing Pad.
12. To configure a **DNISs** Landing Pad, in the left pane, click the **DNISs** folder.
13. Select the **Landing Pads** tab.
14. In the **Name** box, type a name for the DNIS Landing Pad.

15. In the **Number** box, type the number for the DNIS Landing Pad. This number must match the DNIS number configured on the PABX.
16. For SIP Contact Centers, in the **URI** box, type a URI for the DNIS.

    Important:

    The URI must be unique to URIs currently assigned to other DNISs, CDNs, or agents and must not begin with SIP.
17. In the **Service Level Threshold** box, type the time in seconds within which all contacts coming in on this DNIS must be answered or abandoned.
18. In the **Description** box, type an optional description for the DNIS Landing Pad.
19. Click any other row in the grid to save your changes.

Configuring network communication parameters

About this task

Configure the following network communication parameters on each server in the network:

- the number that your telephony PABX dials to route a call to that site
- the number of times your server tries to queue calls to the site after a route attempt fails, and the number of seconds between retries
- the amount of time an agent at the site is reserved to answer a call routed from your server
- the amount of time your server waits for a reply from the remote sites, if routing is based on longest idle agent or average speed of answer
- the Landing Pad type, if the server has Universal Networking enabled

Procedure

1. Log on to the Contact Center Manager Administration client.
2. On the launchpad, click **Configuration**.
3. Select a Contact Center Manager Server nodal site.
4. Select **Network Communication Parameters**.
5. Click **Site Parameters**.
6. From the **Landing Pad Type** list, select the Landing Pad type. Available Landing Pad types depend on the site configuration on the NCC.

   This column is present only if Universal Networking is enabled on the server.

   If you change Landing Pad type, review all timer settings as they can require modifications depending on the selected Landing Pad type.
7. In the **Dialable DN/Prefix** box, type the number that the telephony PABX dials to reach the network CDN at the remote site. The number must include prefixes required by the dialing

plan configured on the telephony PABX. The Dialable/DN prefix value can be up to 32 characters in length.

If you use MCDN networking, enter the number in the format used in your NACD routing table.

You configure the Dialable DN/Prefix field differently if you select MCDN as the Landing Pad type than if you select CDN (Route Point) or DNIS as the Landing Pad type. If you select MCDN as the Landing Pad type, you must configure the Dialable DN/Prefix field with the full dialable number to the network CDN at the target. This is the number that the telephony PABX dials to route a call.

8. In the **Number of Retries** box, type the number of times that your server attempts to route a call to a reserved agent at this site before filtering the site from the routing table.
9. In the **RetryTimer (Sec.)** box, type the time that elapses before the server attempts to queue a call to this site after a route attempt fails (for example, if all trunks are busy).
10. In the **Agent Reserve Timer (Sec.)** box, type the number of seconds an agent at this site is reserved when your site attempts to send a call. If the source site cannot cancel the agent reservation, then it expires after this period.

    Make sure that the Agent Reserve Timer allows enough time for calls to be networked at the destination. Make several test calls to a network skillset that has only one agent logged on at the destination site, and then run a report to ensure that the number of times the agent is reserved is equal to the number of network calls answered. If the number of times the agent is reserved is greater than the number of network calls answered, then the reservation timer is probably too low. Increase the agent reservation timer and make the test calls again.

    The Agent Reserve Timer also applies to the source site if it uses either the Longest Idle Agent or Average Speed of Answer feature and network skillsets are configured with include local node enabled.
11. For the source node only, in the **Nodal Request Wait Timer (Sec.)** box, specify the length of time to wait for responses from destination servers, if the skillset is configured for longest idle agent or average speed of answer. Normally, all nodes respond before the timer expires; after receiving responses from all destination sites, the local server routes the calls and cancels all agent reservations. If one site is slow to respond, agents remain reserved while the local server waits for the response. This timer determines the length of time the server waits for a response before it routes the call and cancels agent reservations.

    The timer must provide sufficient time to allow most destination sites to respond under normal conditions. However, if the timer is too high, agents at the responding sites are reserved (and thus unavailable to answer calls) for long periods of time.

    You can configure this timer differently for each source site. However, the timer applies to all destination sites to which the source site queues calls.

    The Nodal Request Wait Timer cannot equal or exceed the Agent Reserve Timer for the destination sites (this ensures that agent reservations do not time out before the call can

be routed). Avaya recommends that the Agent Reserve Timer be at least 2 seconds more than the Nodal Request Wait Timer.

12. Click **Submit** to save your changes.

Synchronizing site information

About this task

Synchronize site information that the Network Control Center shares with each Contact Center Manager Server in the network. This information includes:

- sites in the network
- network skillsets
- routing tables

The Network Control Center propagates this information to all sites in the network at the following times:

- when it restarts
- after recovering from a network error (for example, if the connection to a specific site was previously unavailable)
- when you manually synchronize sites

Normally, you do not need to synchronize sites manually. However, if the routing tables at the server do not match the routing tables at the NCC, you can force a manual synchronization rather than wait for the NCC to propagate the changes across the network.

Procedure

1. Log on to the Contact Center Manager Administration client.
2. On the launchpad, click **Configuration**.
3. In the Configuration window, double-click the Network Control Center (NCC) server.
4. Select the **Sites** folder.
5. In the Sites window, in the table, select the row containing the site to synchronize.
6. Below the table, click **Sync Site**.
7. In the Confirmation window, click **Yes**.

   The NCC sends information to the selected site. A message appears in the message pane indicating if the synchronization was successful. The message is also logged in the Audit Trail window.

Adding a network skillset

About this task

Add a network skillset in order to assign agents to network skillsets. Assigning agents to network skillsets is the same as the process to assign agents to local skillsets. The server administrator of each server in the network must perform this task on the server. If a server has a local skillset with the same name as a network skillset, the network skillset replaces the local skillset.

Important:

Avaya Aura® Contact Center supports only network skillsets of a voice contact type.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the launchpad, click **Configuration**.
3. On the system tree in the **Configuration** component, double-click the Network Control Center (NCC) server.
4. Select the **Network Skillsets** folder.
5. In the **Network Skillset Name** box, type the name of the network skillset. Network skillset names must be unique.

   You cannot change the name of a network skillset. To change a skillset name, you must delete the skillset, and then add it again.
6. In the **Comment** box, type additional information about the network skillset. This field is optional.
7. From the **Routing Method** list, select the type of routing table to use for this skillset—round-robin or sequential.
8. For Networking Method, select one of the following options:

   Select **First Back**. The server routes network calls to the first responding site.

   OR

   Select **Longest Idle Agent**. The server waits the configured time for sites to respond and then routes calls to the site with the highest priority agent and the longest idle time.

   OR

   Select **Average Speed of Answer**. The server waits the configured time for sites to respond and then routes calls to the site with the highest priority agent and the lowest average speed of answer for the skillset.
9. Click another row of the table to save the new network skillset.

Deleting a network skillset

About this task

Delete a network skillset from the NCC server that is no longer in use.

Note:

After you delete a network skillset on the NCC server the skillset remains on the NCC sites as a local skillset.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the launchpad, click **Configuration**.
3. On the system tree in the **Configuration** component, double-click the Network Control Center (NCC) server.
4. Select the **Network Skillsets** folder.
5. Under **Network Skillsets**, select the network skillset to delete and press **Delete**.
6. On the **Confirm Delete** dialog box, click **Yes**.

Configuring network skillset properties

About this task

Configure the following properties for each network skillset on each nodal site:

- the maximum number of calls that can be queued for the skillset at this server
- the number by which queued calls must decrease before filtering stops
- whether to queue calls to the local site

In addition, if you use the Longest Idle Agent feature, you must make sure that you configure the Agent Order Preference in the Global Settings the same way on every network server.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the launchpad, click **Configuration**.
3. On the system tree in the Configuration component, select a CCMS nodal site
4. Select **Skillsets**.
5. In the **Call Request Queue Size** box, type the maximum number of calls that can be queued for this skillset on your server. For example, if this value is 100, then up to 100 calls can be queued for this skillset at your server. When 100 calls are queued, your server is filtered from the routing tables for this skillset at every other site that attempts to queue a

call for this skillset to your site. If the Call Request Queue Size is zero (0), then no calls are networked in from other sites.

6. In the **Flow Control Threshold** box, type the number by which queued calls for this skillset must decrease before filtering of your server stops. For example, if Call Request Queue Size is 100, and Flow Control Threshold is 20, then filtering of this network skillset ceases only when the number of queued calls falls to 80.
7. Select the **Include Local Node** check box to queue calls to the local node, as well as to remote nodes, with the Queue to Network Skillset command.
8. Click another row of the table to save the changes.

Configuring Agent Order Preference

About this task

Configure the Agent Order Preference for networked sites in your contact center to select the preference. For example, if two agents are available, you can choose the agent closest to the original location of the contact.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the launchpad, click **Configuration**.
3. In the left pane, click **Global Settings**.
4. From the **Agent Order Preference** list, select one of the following:

   Longest total time in idle state since login—Choose this option if you want calls presented to the agent who accumulated the most idle time since logging on.

   OR

   Longest time in idle state since last status change—Choose this option if you want calls presented to the agent who accumulated the most idle time since their last status change.

   OR

   Longest total time since last CDN/ACD call—Choose this option if you want calls presented to the agent with the longest elapsed time since handling a CDN/ACD call.
5. Ensure that Agent Order Preference is configured identically on each server in the network.

Configuring the routing tables

Before you begin

- Add network skillsets.

About this task

When you configure a site, you define a routing table for each network skillset at that site. A routing table defines the sites to which scripts using network skillsets route calls.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the launchpad, click **Configuration**.
3. In the left pane, expand the Network Control Center (NCC) server.
4. Select the **Sites** folder.
5. From the table in the Sites window, select the site to configure
6. In the **Network Skillsets** table, click the skillset to configure.
7. In the **Network Sites** table, select the check box beside each site to which to route calls for this skillset.

   You can add up to 20 sites to a routing table.
8. To arrange the routing order, select a site, and then click the up and down **Rank** arrows.
9. After you arrange all the sites in the routing table for this skillset, select the next skillset to configure.
10. Follow step 5 on page 184 to step 9 on page 184 for each skillset to include in the routing table.
11. Click **Submit** to immediately activate the routing table for this site.
12. To save the routing table as an assignment, click the black triangle beside the Save/ Schedule Routing Table Assignments heading.

Configuring routing table assignments

Before you begin

Important:

If you create an assignment from the NCC using a client, you must select all network skillsets for the source site and reconfigure the routing tables. If you do not select a network skillset that is supported by the source site, when you run the table routing assignment, the Site properties routing table is overwritten with a blank routing table.

About this task

Create a routing table assignment or a new routing table assignment or use another assignment as a template to create the routing table assignment.

Each assignment applies only to the site for which it is defined.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the launchpad, click **Configuration**.
3. In the left pane, expand the Network Control Center (NCC) server.
4. Select the **Sites** folder.
5. From the table in the Sites window, select the site to configure.

   The CDN Landing Pad and DNIS Landing Pad columns appear only if Universal Networking is enabled on the NCC and for at least one site. If Universal Networking is not enabled on a site, the CDN Landing Pad and DNIS Landing Pad check boxes are disabled.
6. In the **Network Skillsets** table, click the skillset to configure.
7. In the **Network Sites** table, select the check box beside each site to which to route calls for this skillset.

   You can add up to 20 sites to a routing table.
8. To arrange the routing order, select a site, and then click the up and down Rank arrows.
9. After you arrange all the sites to include in the routing table for this skillset, click the next skillset to configure.
10. Repeat step 6 on page 185 to step 9 on page 185 for each skillset to include in the routing table.
11. Click **Submit** to immediately activate the routing table for this site.
12. To create a routing table assignment, click the black triangle beside the Save/Schedule Routing Table Assignments heading.
13. In the **Save Assignment as** box, type the name of the assignment.
14. In the **Comment** box, type additional information about the assignment.
15. Perform one of the following tasks:

    To save the routing table assignment, go to step 21 on page 186.

    OR

    To schedule the assignment to run at a future time, from the Schedule Task list, select the type of schedule to create. You can choose from Specific date, Daily, Weekly, and Monthly.
16. From the **Start Time** list, select the time for the schedule to begin.

Important:

The time values represent the application server time, not the client time. If your application server is in a time zone different from the client for which you are scheduling the assignment, you must consider the time difference.

17. To view the current application server time, click **Update** beside the **Application Server Time** box. The schedule that you define must be based on this application server time.
18. In the **Start Date** box, click the button to view a calendar.
19. In the calendar, click the date when you want the schedule to begin.
20. Based on the schedule type (that is, daily, weekly, or monthly), select the days and months when you want the assignment to occur.
21. Click **Save Assignment** to save the assignment.
22. Perform one of the following tasks.

    Click **Yes** to create the reset assignment.

    OR

    Click **No** if you do not want to create a reset assignment.
23. Click **Schedule** to make the assignment effective.

Configuring the historical statistics collection

About this task

Configure the historical statistics collection to specify the length of time network call-by-call statistics are stored on the Network Control Center server.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the launchpad, click **Configuration**.
3. In the left pane, expand the Network Control Center (NCC) server.
4. Click the **Network Historical Statistics** folder.
5. In the **Keep Network Call-by-Call data for** box, specify the number of days to store call-by-call statistics on the NCC.

   This value must match the value configured in the Historical Statistics Configuration window on each server. For example, if you retain network call-by-call statistics for three days, but you retain call-by-call statistics for two days at each site. When you generate a network call-by-call report, the report contains information about events occurring at the destination site, but it does not contain information about events occurring at the source site.

6. In the **Network call rate** box, estimate the average number of calls networked out (routed from one site to another) per hour.
7. Click **Submit**.

   The system calculates the amount of disk space required for the call-by-call database under your configuration. This amount appears in the Required box. The available disk space appears in the Actual box.

Configuring MCDN network CDNs

Before you begin

Important:

Use the MCDN network CDN for incoming network calls only. To check whether local calls are arriving on an MCDN network CDN, use the Network Call intrinsic, and then give the local call a special treatment, such as a RAN route that gives the number to dial for local calls. For more information, see *Using Contact Center Orchestration Designer*.

- Configure the CDNs on the telephony PABX. At the telephony PABX, each CDN is configured like a local CDN; MCDN network CDNs have no special requirements. For information about configuring a CDN on the telephony PABX, see the *Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration*.

About this task

Configure the MCDN network CDN for your server. On each server in the network, you must configure the MCDN network CDN on which incoming network calls are received when using MCDN NSBR.

You can configure multiple MCDN network CDNs for the following reasons:

- To enable agents to identify the source site from the phone display. For example, if all calls from Boston arrive on the MCDN network CDN 555-7777, then when this number appears in the telephone display, the agent knows that the call was sent from Boston. This information can help the agent determine how to respond to the caller. For information about configuring telephone displays, see the Contact Center Manager Administration online help.
- To generate CDN statistics on a per-site basis. You can use network reports to view which source sites are networking calls in to your site.
- To set up treatments for calls from source sites that are returned to the queue before they are presented to an agent. Calls can be returned to the queue if an agent becomes unavailable (by pressing Not Ready, for example) in the moment between arrival of the call at the site and presentation of the call to the agent. For example, you can give RAN messages to callers from various source sites who are routed to the target node and are waiting for an agent to answer.

To use multiple MCDN network CDNs, you must configure a CDN for each server from which you receive calls and configure each server to route calls to a different MCDN network CDN.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the launchpad, click **Configuration**.
3. Select a Nodal CCMS server.
4. In the left pane, click the **CDNs** folder.
5. In the **Name** box, type the name of the CDN as it appears in the CDNs window and on reports.
6. In the **Number** box, type the CDN number as configured on the telephony PABX. This number is the dialable DN that other sites must use to send network calls to your site. To recognize where incoming network calls arrive from, you can set up a separate MCDN network CDN for each site from which you can receive calls.
7. From the **Call Type** list, select **MCDN Network**.
8. Select the **Acquired?** check box to acquire this CDN.
9. Click another row of the table to save the new CDN.

Configuring DNIS Network CDNs

Before you begin

- Configure the DNIS Network CDNs on the telephony PABX. At the telephony PABX, each CDN is configured like a local CDN; DNIS Network CDNs have no special requirements. For information about configuring a CDN on the telephony PABX, see *Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration*.

About this task

Follow the procedure in this section to configure the DNIS network CDNs for each server in the network when Universal Networking is enabled. You must configure the DNIS network CDN on which incoming network calls are received on a DNIS Landing Pad for each server in your network.

You can configure only one DNIS network CDN on each server.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the launchpad, click **Configuration**.
3. Select a Nodal CCMS server.
4. In the left pane, click the **CDNs (Route Points)** folder.
5. In the **Name** box, type the name of the CDN as it appears in the CDNs window and on reports.

6. In the **Number** box, type the CDN number as configured on the telephony PABX. Ensure that this number matches the CDN number configured on the telephony PABX.

   The DNIS Landing Pads on the telephony PABX must map to the DNIS Network CDN. For information about mapping Landing Pads, see *Avaya Aura® Contact Center and Avaya Communication Server 1000 Integration*.

7. From the **Call Type** list, select **DNIS Network**.
8. Select the **Acquired?** check box to acquire this CDN.
9. Click another row of the table to save the new CDN.

Part 6: Communication Control Toolkit

- Communication Control Toolkit fundamentals on page 191
- Resource bulk management on page 194

Chapter 20: Communication Control Toolkit fundamentals

Communication Control Toolkit (CCT) is a client/server application that helps you implement Computer-Telephony Integration (CTI) for installed and browser-based client integrations. This chapter provides some background information for Communication Control Toolkit and the Communication Control Toolkit based applications.

Automatic Call Distribution

Automatic Call Distribution (ACD) is a set of feature packages based on software that provides call distribution in a contact center environment. Some of the features include the following:

- The ability to setup one main number and distribute the calls to a group of agents.
- The ability to set up a supervisor position for an ACD group.
- The ability to monitor the quality of the service provided to incoming callers.
- The ability to gather information about the calls such as, hold time, time in queue, and the number of agents logged in a queue.

Communication Control Toolkit provides a separate application called ACDProxy Service. This application allows the agents to log on, log off, go ready, or go not ready. ACDProxy Service also registers the ACD Queue numbers so an application need not start prior to an agent logs on to a queue. Avaya supports the following ACD features:

- Login or Logout
- Ready or Not Ready
- Make set busy
- Make set in service

Communication Control Toolkit Administration Console

The Communication Control Toolkit Console is a Microsoft Management Console component that is used for server-side and bulk configuration tasks.

Communication Control Toolkit Web Administration

The CCT Web Administration provides the day-to-day administration interface for the CCT product. It allows the Administrator to modify user accounts and other resources required for configuration of CCT. For more information about the day to day management of CCT using the CCT Web Administration, see *Avaya Aura® Contact Center Client Administration*.

Note:

You must run Internet Explorer in compatibility mode for Contact Center Manager Administration and Communication Control Toolkit.

Trace Control Utility

You can use the common logging Trace Control Utility to track trace information to diagnose problems, to provide information to technical support, and to verify method calls and operations.

Programming interfaces

When you configure CCT, your CCT users log on with user accounts based on Windows Active Directory/Domains user accounts.

CCT users are configured in the users and groups section of the CCT Web Administration. To use accounts on the CCT server, the CCT software must be installed using an administrator account on the CCT server. In this scenario the user name has the format <domainname>\<username>.

Users who can access multiple domains can also access the CCT client as long as trust is established between the domains; the user does not have to log on to separate domains to use the CCT client.

Application programming interface

CCT is software for installed and browser-based client integrations. CCT delivers a single cross-portfolio multichannel Application Programming Interface (API) that facilitates the integration of Self-Service and Avaya Aura® Contact Center solutions for your client applications.

The Application programming interface (API) is published as Microsoft .NET types and is distributed as a Windows assembly, which is referenced by application developers.

You can use CCT as next generation computer telephony integration (CTI) middleware and a next generation CTI toolkit. On the client, the API provides a set of interfaces, collectively known as the full Communication Control Toolkit API .

The full Communication Control Toolkit API provides easy access to a subset of CCT functions, which you can use for CTI functionality without having low-level CTI knowledge for the simple development of powerful integrations and applications such as

- desktop applications (for example, Call Control Toolbar)
- server applications (for example, Avaya Call Recording or Work Force Management)
- screen-pop utilities
- business application or Computer Resource Management (CRM) connectors

For more information about using the CCT API, see the Avaya Communication Control SDK Programmers Reference Guide. The Avaya Communication Control SDK Programmers Reference Guide is a help file that accompanies the Software Development Kit. You must join the developer partner program and purchase the Communication Control Toolkit SDK to download the documentation from www.avaya.com.

Web services

The CCT Open Interfaces is a development environment that offers functionality similar to the CCT SDK but provides you with the flexibility of choosing your own development environment. The CCT Open Interface offers a series of service definitions using WSDL, which allows you to choose functionality similar to what is offered by the CCT .NET API.

You can use these services to recreate Agent tools within your own applications or alternatively access call control functionality for Contact Center from any business process.

For more details, see the SDK documentation.

Communication Control Toolkit Reference Client

The Reference Client is an application installed automatically on the Communication Control Toolkit server that mimics a phone device. You can use the Reference Client to simulate making phone calls, transferring phone calls, and other phone events to test the functionality of the Communication Control Toolkit database.

Use the Reference Client to verify calls on one PABX or calls transferred between PABXs.

Chapter 21: Resource bulk management

You use the Communication Control Toolkit Console application on the CCT server to import CCT resources from external sources. You can also use the Communication Control Toolkit Console Bulk Provisioning Tools to import or export CCT resources in large quantities.

The following tools are available:

- Data Import/Export—Imports any or all configuration information from XML files or exports current configuration to an XML file.
- Import CS 1000 Data—Imports CCT terminal and address resource configuration from a Communication Server 1000 capture file.
- Import Windows Users—Imports CCT users from Windows user accounts from either the local machine or the domain in which the CCT Server exists.
- Import Workstations—Imports CCT workstations (computers) from the domain in which the CCT Server exists.

Important:

When any bulk operation is actively importing data into the CCT database, manual configuration changes made through the CCT Web Administration interface are blocked.

Prerequisites to resource management

Procedure

Understand the licensed features for your contact center. Specific resource or resource types can be excluded from your license package.

Importing Windows users

Before you begin

- Ensure that the local administrator has user access for the domain where Communication Control Toolkit is installed to access and import domain resources in the CCT Console.

About this task

Import Windows users from the server to the Communication Control Toolkit database using the Import Windows Users tool. After the resources are in the CCT database, you can configure the resources in the CCT Web Administration client.

To import users from a domain, you must be logged in to the Communication Control Toolkit server using a domain account in the domain from which you wish to import.

If you import domain users configured using the domain.companyname.com format, the CCT import tool imports the user in the domainname\username format.

The Import Windows Users tool is limited to finding at most 999 users. If the search finds more than this number of users only the first 999 users are displayed. To get around this you must select a search type that allows you to filter the results.

Procedure

1. Log on to the Communication Control Toolkit server.
2. On the **Apps** screen, in the **Avaya** section, select **CCT Console**.
3. Expand **Communication Control Toolkit.**
4. Expand **Bulk Provisioning Tools**.
5. Select **Import Windows Users**.
6. In the **Location** box, select the domain or server on which you want to look for Windows users.
7. In the **Search Type** box, select the group of users you want to display. You can look for **All Users**, **Login Name**, **First Name**, **Last Name**, or **Organizational Unit**.
8. In the **Begins With** box, which only appears once **Login Name** or **First Name** or **Last Name** is selected, type the text to use in a search for Windows Users.
9. In the **Actions** pane on the right hand side, select **Search For Users.**
10. In the **Search Results** box, select the Windows users you want to import.

    To select multiple users, press the `Ctrl` key while you select each user. To select all Windows users, click **Add All**.
11. Click **Add**.
12. In the Actions pane, select **Import Selected Users**.

Variable definitions

Name	Description
Search Type	The criteria for selecting a small group of Windows user accounts to import to the Communication Control Toolkit.

Table continues…

Name	Description
	You can choose one of the following options: • Find All Users—find all Windows user accounts on the CCT server. • Login Name—find all Windows user accounts where the user name or logon ID matches or contains the value in the Begins With box. • First Name—find all Windows user accounts where the first name matches or contains the value in the Begins With box. • Last Name—find all Windows user accounts where the last name matches or contains the value in the Begins With box.
Begins With	A string of characters to match in the search for the selected Search Type.

Importing Avaya Communication Server 1000 data

Before you begin

- Establish a terminal emulator connection from a server (not the Communication Control Toolkit server) or workstation to the PABX. The terminal emulator must be capable of capturing text.
- Know the user ID and password to log on to the Avaya Communication Server 1000.
- Apply all Avaya Communication Server 1000 patches, specifically patch MPLR26704. Patch MPLR26704 significantly reduces the time to import address and terminal information into a text file. Only information that is relevant to Communication Control Toolkit is imported.
- Only PABX keys that are AST and IAPG enabled are imported.

About this task

The CCT Import Avaya Communication Server 1000 Data tool allows users to do two things:

- Perform the first step of the import process, convert data capture text file to an XML file. This is done by un-checking the **Automatically import data after conversion** checkbox (this is checked by default).
- Perform both steps of the import process, convert text file to XML file and import data to the database. This is done by leaving the default setting of the **Automatically import data after conversion** check box.

Converting the text file to an XML file allows you to carry out testing of the data import facility without modifying the database contents and enables you to postpone the actual import of the data to an off peak time. The intermediate XML data file generated can be imported at a later stage using the CCT Data Import/Export Tool, by selecting the Standard XML format option.

Before importing the Avaya Communication Server 1000 data to CCT, you must first retrieve the data from the switch. To do this, capture the Avaya Communication Server 1000 data required to configure Communication Control Toolkit to a text file.

Do not use the Communication Control Toolkit server to import the information directly from the switch.

Procedure

1. On a client computer, use the terminal emulator to connect to the Avaya Communication Server 1000.
2. Configure the terminal emulator to capture text, and specify a location for the text file.
3. At the Avaya Communication Server 1000 prompt in the terminal emulator, type `logi admin1` to log on to the PABX.
4. Type your user ID and your password for the switch.
5. If the prompt is not present, continue to press `Enter` until the prompt appears.
6. On the terminal emulator, start the capture text function.
7. Type these commands at the following prompts:

   ```
   >LD 20
   REQ: PRT
   TN: TNB
   TN: Press enter
   CDEN: Press enter
   CUST: 0 (or the customer number)
   DATE: Press enter
   PAGE: ON
   DES: Press enter
   ```

   Downloading information from the Avaya Communication Server 1000 overlay can take a several minutes.
8. To return to the prompt, enter `****` (Shift + 8888).
9. Press `Enter`.
10. If you want to monitor CDNs for custom applications, type these commands at the following prompts:

    ```
    >LD 23
    REQ: PRT
    TYPE: CDN
    CUST: 0 (or the customer number)
    CDN: Press enter
    ```

    The information is downloaded from the overlays.
11. On the terminal emulator, stop the capture text function.
12. Type `logo`.
13. Copy the text file to the Communication Control Toolkit server.
14. Log on to the Communication Control Toolkit server.
15. On the **Apps** screen, in the **Avaya** section, select **CCT Console**.

16. Expand **Communication Control Toolkit**.
17. Expand **Bulk Provisioning**.
18. Select **Import CS 1000 Data**.
19. Select **Passive** for the Avaya Communication Server 1000 Provider.
20. Select **Input File**. This opens a file explorer to select the Avaya Communication Server 1000 data capture file you created.
21. Select the Avaya Communication Server 1000 data capture file, click **Open**. A default path and file name is shown in **Output file**, change this if necessary.
22. To import the data into the database select **Automatically import data after conversion.**
23. In the **Actions** pane on the right hand side, select **Convert/Import**. A progress bar in the Status area indicates the progress made by the tool in three phases:
    - Conversion of the data capture file
    - Generation of the output file
    - Import of the data into the database
24. The status area displays data imported and the conversion results, including the number of TNs, DNs, and CDNs found. If applicable, a list of errors is also displayed. This list includes line numbers where the errors were discovered in the supplied data capture file.

    Important:

    An error dialog shows errors in the conversion step. The error dialog appears prior to beginning the automatic import. The user can choose to cancel the import step or proceed.

Next steps

The conversion process adds all terminal and CDN information downloaded from the CS 1000 PABX to the Symposium TAPI SP database. Some of this information is not required for Contact Center. Use the CCT WebAdmin tool to remove imported TNs and Addresses that are not used by contact center agents or by custom applications. Then remove CDNs that are not used by custom applications.

Importing workstations from the domain

Before you begin

- A local administrator must have access to the contact center domain to import domain resources to the CCT Console. Domain resources that can be imported are domain users and domain workstations. Ensure the local administrator has access to the contact center domain.

About this task

All Contact Center applications are in a contact center domain. Import workstations from the contact center domain to the Communication Control Toolkit server using the Import Workstations tool.

To import workstations from a domain, you must be logged in to the Communication Control Toolkit server using a domain account in the domain from which you wish to import. If logged in as a local administrator the Import Workstations tool is not available.

The Import Workstations tool is limited to finding at most 999 workstations. If the search finds more than this number only the first 999 are displayed. Therefore, you must select a search type that allows you to filter the results.

Procedure

1. Log on to the Communication Control Toolkit server.
2. On the **Apps** screen, in the **Avaya** section, select **CCT Console**.
3. Expand **Communication Control Toolkit**.
4. Click **Import Work Stations**.
5. Set **Search Type** to **All Workstations**.
6. Select the workstations to import from the **Available Work Stations** list.
7. Click **Add**.
8. Click **OK**.

Variable definitions

Name	Description
All workstations	All workstations in the domain are returned, up to a limit of 1000.
Name Contains	Workstations whose names contain the specified string (case insensitive) are returned.
Name begins with	Workstations whose names begin with the specified string (case insensitive) are returned.
Name ends with	Workstations whose names end with the specified string (case insensitive) are returned.

Importing bulk resources

Before you begin

- Ensure that you have an XML file that matches the required file format to import the resources into the Communication Control Toolkit database.

About this task

Import bulk resources into the Communication Control Toolkit database using the Data Import/Export Tool of CCT Administration Console.

Resources can be imported from a standard XML file or a flattened XML file. Use a flattened XML file with Microsoft Excel because Microsoft Excel limits the depth of the XML nodes by representing complex data stored in the database as strings.

The Data Import/Export Tool replaces the Import Configuration tool in the last release. Because of changes made to the database schema, the file formats (both TAB and XML) used in the previous release are not compatible with the Contact Center Database Import/Export tool.

You can use the Data Import/Export Tool while CCT is processing calls. Import and export operations initiated through this tool are performed in the background and do not require that the CCT Administration Console be left running. However, when a bulk provisioning operation is in progress, no manual configuration updates can be performed until the bulk operation completes or is cancelled (using this tool).

Procedure

1. Log on to the Communication Control Toolkit server.
2. On the **Apps** screen, in the **Avaya** section, select **CCT Console**.
3. In the CCT Console window, expand **Communication Control Toolkit**.
4. Expand **Bulk Provisioning Tools**.
5. Click **Data Import/Export Tools**.
6. In the **Format** drop-down box, select **Standard XML** or **Flattened XML**.
7. In the **Actions** pane select **Import**, a file explorer window is displayed.
8. Browse to and select the file to import, select **Open**.

   The data in the file is imported and the Status and Total Records Imported are shown in the status pane.
9. Use the CCT Web Administration to view the imported data.

Exporting bulk resources

About this task

Export bulk resources from the CCT database using the Data Import/Export tool of the CCT Snap-in. For data analysis, export resource configuration data and the resource assignments to a single file.

Resources can be exported to a standard XML file or a flattened XML file. Use a flattened XML file with Microsoft Excel because Microsoft Excel limits the depth of the XML nodes by representing complex data stored in the database as strings

When a file is exported using the Data Import/Export tool, the schema definition file (XSD file) for the selected export format is created in the output location, along with the requested export file.

The Data Import/Export tool replaces the Export Configuration tool in the last release. Because of changes made to the database schema in Contact Center, the file formats (both TAB and XML) used in the previous release are not compatible with the Contact Center Database Import/Export tool.

Procedure

1. Log on to the Communication Control Toolkit server.
2. On the **Apps** screen, in the **Avaya** section, select **CCT Console**.
3. In the CCT Console window, expand **Communication Control Toolkit**.
4. Expand **Bulk Provisioning Tools**.
5. Click **Data Import/Export Tools**.
6. In **Setup**, select **Standard XML** or **Flattened XML** in the Format drop down box.
7. In **Setup**, select the **resources** to export.
8. In the **Actions** pane select **Export**, a file explorer window is opened.
9. Browse to and select the file to save the data to, select **Save**.

   The data in the file is imported and the Status and Total Records Imported are shown in the status pane.

Variable definitions

Name	Description
Mappings	The mappings recorded in the Communication Control Toolkit database between users, terminals, address, agents, user groups, terminal groups, address groups. You can choose all assignments or individual assignments by selecting the appropriate check boxes under Mappings.
Resources	The resources recorded in the Communication Control Toolkit database such as users, terminals, address, agents, workstations, user groups, terminal groups, address groups. You can choose all resources or individual resources by selecting the appropriate check boxes under Resources.

Table continues…

Name	Description
Export File Format	The final output of the exported data. You can choose from two formats: • A standard data schema definition file • A flat schema definition file The difference between the two is that the “flat” schema is suitable for use with Microsoft Excel because it limits the depth of the XML nodes by representing some of the more complex data stored in the database as strings.

Part 7: Contact Center Multimedia

- Contact Center Multimedia fundamentals on page 204
- General configuration on page 224
- Outbound configuration on page 240
- Email configuration on page 242
- Voice mail configuration on page 290
- Scanned document configuration on page 299
- Fax configuration on page 309
- Social Network contact Configuration on page 319
- Instant message configuration on page 326
- Short Message Service configuration on page 332
- Web communications configuration on page 342
- Agent Desktop configuration on page 363
- Data Management - cleanup and purging on page 420
- Data Management - customer privacy on page 433

Chapter 22: Contact Center Multimedia fundamentals

Use the Contact Center Multimedia (CCMM) application to have the contact center accept a variety of contact types and route them to agents who can handle the contact type. The contact types that an agent can handle are determined by the skillsets to which the agent is assigned.

Contact types routed using Avaya Aura® Contact Center include the following:

- voice contacts
- email messages
- Short Message Service (SMS) text messages
- faxed documents
- scanned documents
- Social Networking contacts
- voice mail messages
- outbound contacts
- Web communications contacts
- instant messages (for SIP-based PABXs)

The Contact Center Manager Server and Communication Control Toolkit server handle and route voice contacts. All other incoming contacts pass to Contact Center Manager Server using the Contact Center Multimedia server.

The Contact Center License Manager licenses each contact type. You must have the appropriate license in your contact center to enable routing for the contact type.

You can configure a schedule for the hours your contact center is open.

Log on to Contact Center Manager Administration (CCMA) and select **Multimedia** from the Launchpad to access the Multimedia Administration tool. Some settings on the tool require that you log on to CCMA from a Web browser on the CCMM server. These settings are:

- Agent Desktop Configuration
  - General Settings
  - Basic Screenpops
  - Advanced Screenpops

- User Settings
- Shortcut Keys

• E-mail

- General Settings - Advanced

Note:

You configure Activity codes, Not Ready Reason codes, and After Call Work Item (ACW) codes using Contact Center Manager Administration Configuration. For more information, see *Avaya Aura® Contact Center Client Administration*.

Email contact type

Use email messages to communicate with clients by using an email provider such as Microsoft Exchange.

You can route email contacts by using rule groups based on specific information you configure for the contacts. The Email Manager routes incoming contacts based on the address where the email message is received, the text in the email message, or the email address that sent the email message. The email message is assigned to a skillset with a priority, and then routed to an agent who can handle the contact based on the received criteria.

The email contact type has several components:

- Email rule groups on page 206
- Recipient mailboxes on page 206
- Inbound email settings on page 207

You must configure email settings for email messages leaving your contact center as a campaign or in response to customer email messages.

- Outbound email settings on page 207
- Character encoding for outgoing email messages on page 207

You can configure the email message contact type for international languages, see Asian email on page 208.

You can view real-time traffic reports for your email messages. Configure the date and time for which you want to review the email traffic in your contact center. See Email traffic reports on page 208.

You can enable the Extended Email Capacity feature if you require the email backlog capacity to be more than 20 000. The Extended Email Capacity feature increases the email backlog capacity to 100 000 contacts. For more information, see Extended Email Capacity on page 209.

You can configure the Supervisor Email Approval feature so that supervisors can approve email messages before they reach the customers.

Note:

The approval process applies to email contacts only and does not apply to other contact types such as Fax, Scanned Documents, and SMS.

Based on your quality assurance requirements, regulatory requirements or agent training requirements, some or all of the email messages can be sent for supervisor approval. You can configure email messages targeted for supervisor approval on a per skillset basis or per agent basis. For more information, see Supervisor approval of email messages on page 210.

Agents handle email messages using Agent Desktop. Contact Center Manager Administration manages other real-time and historical reporting. See Agent Desktop on page 212, Contact Center Manager Administration on page 212, and Web services on page 212.

You can develop a custom Web service that the Email Manager can call when an email message is processed. The custom Web service can perform custom tasks such as manipulating the originating email and modifying the rule routing options. For more information, see Open Interfaces for email on page 213.

Email rule groups

Rules determine how a multimedia contact is routed based on information about the email message (input) and configurations in your contact center.

A basic rule considers the first recipient address of the contact and can assign a skillset. You can further enhance the routing by searching for specific keywords in the body of an email or by looking at who sent the message.

Rule groups are collections of rules that evaluate the incoming email and route the contact according to the best match or the first match.

You can also enhance the routing by selecting additional output details for your contact center, such as automatic responses.

By default, one rule group is supplied that contains the default rule for routing an email contact to a specific skillset with a priority.

For example, a magazine advertises an investment strategy. Customers can learn more about the investment by sending an email with “Good Investing” in the subject line to a specific address. Create a rule to search incoming email messages for “Good Investing.” If the email subject line contains this subject line, then a brochure is sent to the customer. No interaction from an agent is required. The rule group “investments” is applied to the recipient mailbox at which the email message is received.

Recipient mailboxes

Contact Center Multimedia polls specific recipient mailboxes on the email server based on a list of mailboxes defined in the Multimedia Administrator recipients list. The email retrieved from these

mailboxes is routed based on defined rules applied to either a mail store or an alias. You must ensure that enabled email addresses configured in your Email Manager are already configured on your corporate email server.

The recipient mailbox has a default rule group assigned to handle the email messages, but you can assign a custom rule group to the recipient.

Recipient mailboxes also receive messages from other contact types. Voice Mail contacts attach a .wav file. Faxes and scanned documents attach a .tiff file to an email message handled by the Email Manager. An SMS text message also uses the Email Manager to route text messages.

Inbound email settings

Perform this optional configuration if you are licensed for email contacts.

You can configure the following optional email settings:

- how frequently you scan the email server for new messages
- the location in which to store attachments
- the text searched when you use keywords for rules

Outbound email settings

Configure outgoing email mailbox settings to identify who responds to the email message from the customer. For outgoing email, you can change the character encoding of the message to display the email message with the correct characters.

The response can contain the email address to which the customer sent the original email message or a general corporate email address configured for each skillset. Agent-initiated messages are always sent from an email address associated with a skillset.

Email messages must be relayed through the email server, not forwarded to another party if you manage email messages on behalf of an external source. Sending email messages preserves the original To address that is used for email rule administration and outgoing email addresses.

Character encoding for outgoing email messages

The Contact Center Multimedia Email Manager replies to an email message using the same characters as the inbound email. For example, if an email arrives to the contact center with Latin-1 encoding, the reply from the Agent Desktop or the automatic response is sent in Latin-1. The customer email client can understand the format of the message sent from the contact center.

If the customer sends an email message in English and receives either an agent response or an automatic response in another character set, you cannot tell if the customer email client can decode the new character set. Avaya recommends that if you use an automatic response, you use

rules to search for words in the expected languages (for example, Japanese or English) to ensure that the response sent matches the language of the inbound email.

If the original email is encoded with the Latin-1 character set (ISO-8859-1), you can choose to reply in Latin-9 character set (ISO-8859-15) to provide support for the Euro Currency Symbol. The Euro Currency Symbol is not included in the Latin-1 character set, instead, it is represented by a question mark (?). Not all recipients understand the Latin-9 character set, and the reply email can be perceived as a blank email. Avaya recommends that only contact centers in Europe use Latin-9 encoding.

Asian email

Internationalized domain names (IDN) can include characters from East Asian languages. Using characters from East Asian languages is dangerous because this can be used by phishing sites. Phishing is a way of attempting to acquire information such as names, passwords, and credit card details by misrepresenting a malicious website as a legitimate website.

Phishing email messages contain links to malicious websites that look similar to legitimate business websites. For example, the IDN of a phishing site can achieve this by replacing Latin 1 characters with East Asian characters that are visually similar or identical.

The World Wide Web Consortium uses punycode to implement IDNs. Punycode is an ASCII equivalent to the domain name. Normally, the client (Web browser or email client) accepts the IDN in native characters and converts it to punycode; for example, xn--jp-cd2fp15c@xn--fsq.com. The receiving client identifies the sender as being a punycode string and interprets the native characters.

Contact Center Multimedia supports IDNs. You or a customer can enter a punycode email address. The receiving client can render the native characters.

Email traffic reports

Reports appear in the CCMM Administration utility to show the current status of the email traffic. The following reports appear when you select E-mail in the left column of the Multimedia Administrator application. You can choose the report date and the skillsets represented in all displayed real-time reports.

- E-mail (New Vs. Closed) shows the number of contacts in a new and closed state against the time for the selected date and skillsets. You can use this report to monitor the incoming and closing rate for email and to determine if the traffic levels are adequately managed. The number of new contacts is defined as those with an arrival time since midnight on the selected date. The number of closed contacts is defined as those with a close time since midnight on the selected date.
- E-mail Progress shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for that date.

- E-mail Closed Contacts Queue Time shows the average time an email contact spends in the queue while the contact center is open. The queue time is defined as the time between when the contact arrives in the contact center and the time the contact is presented to an agent less the time that the contact center is closed. This report shows only closed contacts for the selected date, and reflects only a partial summary of the service level achieved for the date.

Extended Email Capacity

Currently, the maximum capacity of Open Queue is 20 000 contacts. Email Manager observes the current number of contacts queued and stops processing email messages from the mail server after the number of contacts reaches the upper limit.

The Extended Email Capacity feature increases the email backlog capacity to 100 000 contacts. Contact centers that have large email volumes can use the Extended Email Capacity feature to pull email messages that are present in the CCMM database. Agents can then view email contacts in the CCMM database and search or extract these contacts, while on a voice call with a customer.

Email Scheduler Service is a new Contact Center Multimedia (CCMM) service. This service monitors the Real-time Statistics Multicast (RSM) stream and multimedia database for skillset statistics corresponding to email skillsets. This service gathers the following information:

- The skillsets in service.
- The number of available agents. The CCMM database provides the number of in-service agents.
- The number of queued contacts. RSM provides information about the Calls Waiting statistics.

Email Scheduler Service uses this information to ensure that sufficient contacts are queued on each skillset.

Note:

Generally, the system queues two contacts per logged in agent on a skillset. However, in certain circumstances the actual amount of contacts queued can be more.

By default, the Extended Email Capacity feature is disabled. If you require the email backlog capacity to be more than 20 000, you must enable this feature.

If the Extended Email Capacity feature is disabled, Email Manager performs nightly checks on the number of email messages that have a New status in the multimedia database. If the number of email messages that have the New status is more than 10 000 in a standalone CCMM configuration and 4 000 in a coresident configuration, Email Manager sends an email to the administrator to enable the Extended Email Capacity feature. You can configure the distribution list for this email in CCMM Dashboard. For more information, see Adding an email address of an administrator in CCMM Dashboard on page 283. Email Manager uses the address assigned to the EM_Default_Skillset as the From Address. If you do not configure this address, Email Manager sends the notification to a dummy address, which triggers a delivery failure notification. The delivery failure notification then routes to an agent. The text of the email is set up as a prepared response with a default System Message.

On CCMM Dashboard, you can see whether the Extended Email Capacity feature is enabled. If the Extended Email Capacity feature is disabled, and the number of New email contacts in the CCMM database is more than 10 000 in a standalone CCMM configuration and 3 000 in a coresident configuration, the dashboard displays an amber warning icon to the left of the “Extended e-mail capacity status” label.

If the number of New email contacts in the CCMM database is more than 15 000 in a standalone CCMM configuration and 4 000 in a coresident configuration, the dashboard displays a red warning icon to the left of the left of the “Extended e-mail capacity status” label.

For information about enabling the Extended Email Capacity feature, see Enabling Extended Email Capacity on page 284.

Note:

The Email Scheduler Service, which handles the rescheduling of email contacts, runs at 10 minute polling intervals. If agents postpone an email for less than 10 minutes, in certain scenarios the email does not reopen precisely at the scheduled time.

Supervisor approval of email messages

Before an email message reaches a customer, supervisors can approve or reject email messages that agents send to customers.

The approval process applies only to email contacts. The approval process does not apply to other contact types such as Fax, Scanned Documents, and SMS.

Configuration of Supervisor approval of email messages

Based on your requirements, the system can send some or all of the email messages to supervisors for approval before the system sends the email messages to a customer.

Quality assurance or Regulatory requirements: You can configure contacts that the system sends to supervisors for approval on a per skillset basis, which means that a percentage (0-100) of email messages sent from a skillset requires approval from supervisors. For more information, see Configuring supervisor approval for email messages on a per skillset basis on page 271.

Important:

For approval of agent email messages, you must configure an approval skillset to which the system sends the agent email messages.

Agent training: You can also configure contacts that the system sends to supervisors for approval on a per agent basis, which means that a percentage (0-100) of the email messages sent by particular agents require approval from supervisors.

For example, you can configure that 100% of the email messages that new agents send require approval from supervisors and 50% of the email messages that agents who have been in the contact center for over six months send require approval from supervisors. For more information, see Configuring supervisor approval for email messages on a per agent basis on page 365.

Agents can pull contacts for approval. You must restrict this by configuring skillset partitions. For more information, see Configuring agent access to contacts on page 365.

Agents cannot request approval of email messages. You cannot configure keywords to trigger the approval process.

You can configure up to five levels of approval from supervisors before email messages reach customers. The system sends email messages through a hierarchy of supervisors before the system grants the final approval.

You can also configure the system to automatically reject email messages from all skillsets based on keyword groups. For more information, see Configuring auto-rejection of email messages from all skillsets that use approval hierarchy on page 273.

Flow of email messages through Agent Desktop

Agent Desktop handles the flow of email messages as follows:

- When an agent sends an email message, the system marks the email message for approval and returns the email message to a predetermined skillset in the queue for approval.

  Supervisors who review the email message that the agent sends to the customer must be assigned to the approval skillset.

  Agents can belong to the skillset that approves email messages. Therefore, you must configure the approval process in a way that restricts agents from approving email messages.
- If the supervisor approves the email message, the system marks the email message to be sent to the customer or returns the email message to the queue if the email message requires further approval. If the email message requires further approval, the system targets the email message to the next approval skillset in the hierarchy.
- If the supervisor rejects the email message, the system marks the email message as rejected and returns the email message to the queue targeted to the previous skillset. The email message flows through the rejection hierarchy till the email message reaches the originator for redrafting. The supervisor must add review comments so that the originator can redraft the email message.

  Only the originator of the email message can edit or redraft the email message. Supervisors at all levels can only add review comments.

The system does not move email messages through the approval hierarchy in the following situations:

- You delete a skillset that is part of the supervisor approval chain and the contact is already in queue waiting for that skillset to come into service
- You delete the original agent and a supervisor rejects the email message
- You delete the supervisor who must approve the email message

In order to handle such contacts, agents must use Agent Desktop to pull contacts.

Agent Desktop

Agents use Agent Desktop to process email contacts. When an email message arrives at the contact center, it is routed to Agent Desktop, and agents can perform the following activities:

- Accept or reject an email message.
- Review and update customer information.
- Create a reply.
- Transfer the contact to an agent, skillset, or expert.
- Select a prepared response to send to the customer contact.
- Select an activity code to record the result of the customer contact.

For more information about Agent Desktop, see the *Using Agent Desktop for Avaya Aura® Contact Center .*

Contact Center Manager Administration

Use Real-Time Reporting and Historical Reporting in Contact Center Manager Administration to create and run real-time and historical reports for email contacts.

For more information about the reporting and performance statistics, see the following documents:

- *Contact Center Performance Management Data Dictionary*
- *Using Avaya Aura® Contact Center Reports and Displays*
- *Avaya Aura® Contact Center Client Administration*

Real-Time Reporting displays real-time and up-to-date statistics information regarding a campaign, such as the number of waiting contacts, the number of answered contacts, or the average answer delay.

Web services

The Open Interfaces provide Web services for integrating third-party agent applications with the Contact Center Multimedia server for the processing of email contacts received into monitored mailboxes.

The Web services provide the following functions for external applications:

- agent authentication with CCMM Database
- ability to read email contacts
- ability to reply to and forward email contacts

For more details, see the SDK documentation.

Open Interfaces for email

You can develop a custom Web service that the Email Manager can call when an email message is processed. The custom Web service can perform custom tasks such as manipulating the originating email and modifying the rule routing options.

The Email Manager retrieves the email from the mailbox and performs keyword analysis on the contents of the email. The keyword analysis sets a particular rule. The rule sets a number of properties such as auto-response, skillset, and priority. While configuring the rule, you can associate a Web service with the rule. The Web service can then perform a custom action and return values that can override the original email, the skillset, or the priority. Using the custom Web service, users can customize email messages and associate properties based on their business needs. You can use the custom Web service to manipulate both the content and the routing of the email message.

The following are some examples of using a custom Web service:

- To mask credit card details at source for Payment Card Industry (PCI) compliance: Inbound email messages can contain credit card numbers, PINs, expiry dates, and CV2 codes. The Web service can match the patterns of credit card numbers, extract the numbers for processing, and then mask the numbers in the email message before presenting the same to an agent.
- To remove obscenities from inbound email messages: Inbound email messages can contain abusive words. The Web service can remove these words from the email message before presenting the same to the agent.
- To extract Custom Tracking IDs for screen pops: An external system generates email messages and inserts tracking numbers in the subject field. A customer receives the automated email and replies with a query. As the format of the tracking number is proprietary, the existing keyword analysis fails to match the tracking number. The Web service can extract the tracking number that can be used to display a screen pop that contains the appropriate record.
- To integrate with the Knowledge Base articles: A custom Web service can find Knowledge Base articles that match the customer queries. The system then displays a screen pop with relevant Knowledge Base articles.
- To integrate with Avaya Aura® Experience Portal multimedia notifications: Experience Portal can send customized email messages or SMS messages in bulk. Based on the email or SMS messages, customers can reply and self service can follow. Self service depends on customer replies that contain keywords. After the customer completed the self service, an agent receives the email message, no context for the self service session is provided to the agent. A custom Web service can extract custom identifiers and query Experience Portal for context, persisting or linking to the context in the multimedia database.

You can use C# or Java to develop a custom Web service. The custom Web service must conform to Web Service Description Language (WSDL) standards.

Note:

You must not host the custom Web service on the Avaya Aura® Contact Center server.

While configuring a custom Web service, you must specify the mapping of the input and output parameters. For example, the Web service might take an input parameter of the email body and return a modified email body as well as the priority for that email. The email processing is based on these output parameters instead of the original values.

Input parameters:

- Mailstore
- To Address
- To Address List
- CC Address List
- From Address
- Subject
- Plain Text Body
- HTML Body
- E-mail headers

Output parameters:

- To Address List
- CC Address List
- Subject
- Plain Text Body
- HTML Body
- Skillset
- Priority
- Customer ID
- CustomField Name
- CustomField Value
- From Address
- Agent ID
- Auto-close

For more information about configuring Open Interfaces for email, see Configuring Open Interfaces for email on page 285.

CCMM Dashboard utility

Use the CCMM Dashboard utility to perform the following tasks:

- Monitor the number of contacts for optimum performance
- Troubleshoot contact routing errors

CCMM Contacts by Type

You can use the CCMM Dashboard utility to monitor the number and state of contacts in the Contact Center database. On the CCMM Dashboard, the “CCMM Contacts by Type” section displays the type, state, and number of contacts in the Contact Center database.

The “CCMM Contacts by Type” section has the following columns:

- Type — The contact type name is displayed in this column. For example, EMail, Outbound, Scanned Document.
- New — The contact is currently in a queue. The new contact has not yet been assigned to an agent.
- Open — The contact is currently presented to an agent. The agent is handling this open contact.
- Closed — The contact was handled and is now finished.
- Waiting — The waiting state is used when the Extended Email Capacity feature is enabled. Contacts that are not added to a queue and or moved to the New state are in the Waiting state.

The “CCMM Contacts by Type” section has a row, labelled “Total”, which displays the total number of contacts in each of the above columns.

You can use this information to monitor the number of contacts for optimum performance.

Routing Search

You can use the CCMM Dashboard utility to troubleshoot contact routing errors.

1. When an email contact is presented to an agent, use the left panel of Avaya Agent Desktop to get the email contact ID number.
2. On the CCMM Dashboard, click Routing Search. The Contact Routing Search screen appears.
3. On the Contact Routing Search screen, in the contact ID box, type the contact ID number of the email contact.
4. Click Search.
5. When the search completes the Contact Details, Association, Rule Details, and Rule Group Associated Email Addresses sections display routing information about the email content.
   - The Contact Details section contains the general information about found contact.
   - The Association section contains the information about To Address associated with any special Rule Group or System Default Rule.

- The Rule Details section shows the rule applied to found contact and skillset name which was used according with this rule.
- The Rule Group Associated Email Addresses section shows what email addresses are applied for the rule used for found contact.

6. To close the Contact Routing Search screen, click Close.

You can use this information to monitor and troubleshoot how Contact Center routes email contacts.

SMS text messages, faxes, scanned documents, and voice mail attachments

The Short Message Service (SMS) text message is a standard communications protocol for the exchange of short text messages between mobile phone devices. SMS messages are forwarded by an SMS gateway to an email address.

A fax (short for facsimile) is a document sent over a phone line. Faxes are forwarded by a fax server to an email address as a .tiff attachment.

A scanned document is an electronic version of a printed page or document. Scanned documents are forwarded by a document imaging server to an email address as a .tiff attachment.

A voice mail is a spoken message including a message on an answering machine. Voice mail messages are forwarded by a voice mail server to an email address as a .wav attachment.

For each type of contact, you can configure the routing of the specified contact and assign a priority to the contact. See Mailbox configuration on page 217.

You can view traffic report summaries for each type of contact. See Traffic reports on page 217.

Use the Agent Desktop to open and reply to SMS, faxes, scanned documents, and voice mail contacts. See Agent Desktop on page 218.

For the previously listed contact types, the Email Manager retrieves the message or attachment and queues it to the default or defined skillset with the assigned priority. For faxes and voice mail attachments, the Email Manager permits the caller ID be extracted to facilitate replies or callbacks.

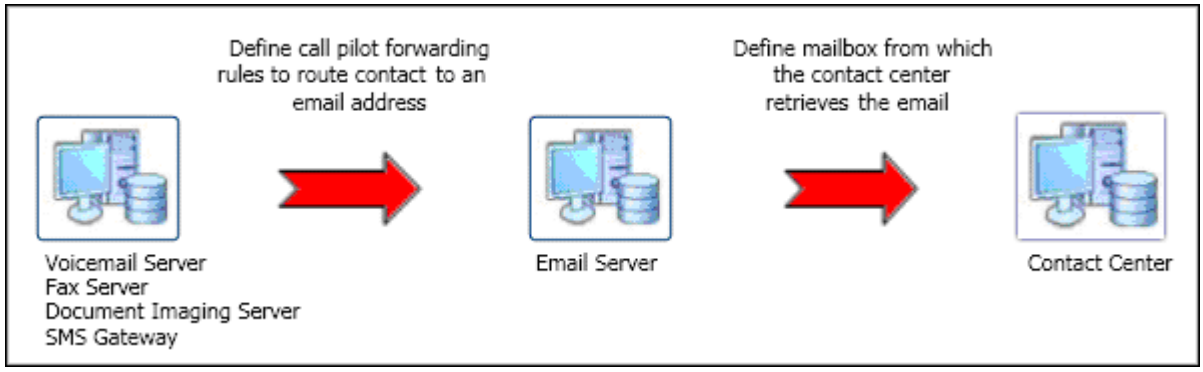


Figure 1: Contacts attached to email cycle

Mailbox configuration

You can configure the following properties for the contacts:

- POP3 or IMAP Server (for receiving email messages)
- recipient mailbox
- password for access to the mailbox
- skillset and priority
- sender address, either full sender address or Calling Line ID (CLID)
- reply address for skillset
- SMTP Server (for sending email messages)
- sending mailbox

Traffic reports

Reports appear in the CCMM Administration utility to show the current status of the contact type traffic. The following reports appear when you select the contact type in the left column of the Multimedia Administrator application. You can choose the report date and the skillsets represented in all displayed real-time reports.

- The New Vs. Closed report shows the number of contacts in a new and closed state against the time for the selected date and skillsets. You can use this report to monitor the incoming and closing rate for contacts of a particular type and to determine if the traffic levels are adequately managed. The number of new contacts is defined as those with an arrival time since midnight on the selected date. The number of closed contacts is defined as those with a close time since midnight on that date.
- The Progress report shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for the selected date.

- The Closed Contacts Queue Time report shows the average time a contact spends in the queue while the contact center is open. The queue time is defined as the time between when the contact arrives in the contact center and the time the contact is presented to an agent less the time that the contact center is closed. This report shows only closed contacts for the selected date, and reflects only a partial summary of the service level achieved for the date.

Agent Desktop

Agents use Agent Desktop to process SMS, faxes, scanned documents, and voice mail contacts. When one of these contacts arrives at the contact center, CCMM routes it to a skillset, and agents can perform the following activities:

- Accept or reject the contact.
- Review and update customer information.
- Create a reply.
- Select a prepared response to send to the customer.
- Select a activity code to record the result of the customer contact.

Outbound contact type

The outbound contact type is an outgoing call made by an agent to a customer, for example, a sales or marketing call.

Contact Center Outbound consists of several components:

- Outbound Campaign Management Tool on page 218
- Campaign Scheduler on page 219
- Agent Desktop on page 219
- Contact Center Manager Administration on page 220
- Web services on page 220

Outbound Campaign Management Tool

Use the Outbound Campaign Management Tool in Contact Center Manager Administration to create, modify, and monitor outbound campaigns.

A contact center administrator or supervisor can use the Outbound Campaign Management Tool to create and monitor outbound campaigns. The Outbound Campaign Management Tool provides the following main functions:

- Define a campaign.
- Import call data.
- Create disposition codes.
- Review outbound call data.
- Create and preview optional agent scripts.
- Review campaign progress.

Campaign Scheduler

This Contact Center Multimedia server component determines when to queue contacts to the Contact Center Manager Server. The Campaign Scheduler monitors the status of each campaign and performs the following actions:

- Assigns the campaign status to running and queues contacts to Contact Center Manager Server when the campaign start time or daily start time occurs.
- Assigns the campaign status to nonrunning and removes contacts from Contact Center Manager Server when the daily end time occurs.
- Assigns the campaign status to expired and removes contacts from Contact Center Manager Server when the daily end time occurs.
- Assigns the campaign status to completed when all contacts are processed.

The Campaign Scheduler queues outbound contacts at the rate required to maintain 5 outbound contacts waiting for each logged in agent on each outbound skillset.

The Campaign Scheduler also queues rescheduled outbound contacts falling due within the next 15 minutes. Therefore the Real Time Display (RTD) for the skillset can show more than 5 times the number of staffed agents, depending on rescheduled outbound contacts falling due within the next 15 minute period.

The RTD can display less than 5 times the number of staffed agents, where there are not enough outbound contacts, which fall within the configured dialing hours based on customer time zone, waiting in outbound campaigns.

Agent Desktop

Agents use Agent Desktop to process outbound contacts. When a campaign runs, outbound contacts are routed to Agent Desktop, and agents can perform the following activities:

- Accept or reject an outbound contact.

- Review and update customer information.
- Make the outbound voice call.
- Follow an agent script and record customers answers and comments.
- Select a disposition code to record the result of the call.

Contact Center Manager Administration

Use Real-Time Reporting and Historical Reporting in Contact Center Manager Administration to create and run real-time and historical reports for outbound contacts.

Real-Time Reporting displays real-time and up-to-date statistics information regarding a campaign, such as the number of waiting contacts, the number of answered contacts, or the average answer delay.

Web services

The Outbound Open Interfaces provide an open interface for integrating third-party applications with Outbound Campaigns.

The open interfaces provide the following functions for external applications:

- ability to add contacts to an existing campaign
- ability to close contacts already created as part of a campaign

The most common use of these interfaces is to automatically load a caller list to an existing outbound campaign.

For more details, see the SDK documentation.

Web communications

Avaya Aura® Contact Center 7.0.1 provides two services for web chat: Web Communications text chat and Enterprise Web Chat (EWC). EWC supports integration with Agent Desktop only with a standalone Multimedia server on a Unified Communications solution. EWC is a licensed feature, and requires a Web Chat SDK license.

Use the Web Communications Manager to communicate with customers over the Internet. Agents and customers directly communicate in real time by conducting a two-way conversation by exchanging text messages using JavaScript- and frame-compliant Web browsers. The Web Communications Manager provides the following functions:

- intelligent routing of customer communications to the agent who has the subject knowledge to respond

- an Agent Desktop interface for agents to respond efficiently to customers
- easy referencing of the thread of conversation between the customer and the agent in a text chat session
- an optional customer-centered multimedia presentation to the customer’s browser while the customer waits for an agent
- push Web pages to the other party during conversations for discussions
- the ability for agents to accept and work on multiple contacts
- the ability for agents to transfer Web Communications contacts to other agents

You must configure the skillset and configure the Web server to configure the Web Communications Manager.

Instant Messaging

The automatic text for an instant message communication includes a welcome message for customers who initiate a session, and a disconnect message for the customer in the text-based conversation. You can configure default instant messages for individual skillsets. Instant messaging is available only in a SIP-enabled environment.

The instant message capability provides the following functions in a SIP environment:

- intelligent routing of customer communications to the agent who has the subject knowledge to respond
- an Agent Desktop interface for agents to respond efficiently to customers
- easy referencing of the thread of conversation between the customer and the agent in a text chat session
- an optional customer-centered multimedia presentation to the customer’s browser while the customer waits for an agent
- push Web pages to the other party during conversations for discussions
- the ability for agents to accept and work on multiple contacts

Office hours

For all delayed time contacts, including email messages, faxed documents, scanned documents, voice mail messages, and SMS, you can configure the office hours for the contact center.

The time that a delayed contact spent in queue includes the time the contact was queued less the time that the contact center is closed. You can configure closed hours for daily operations and holidays in the contact center.

Contact Center Multimedia in a voice-only solution

In a voice-only solution, Avaya Agent Desktop handles only voice calls from customers. Multimedia contacts are not supported. Therefore, in a voice-only solution without multimedia licenses, the CCMM Administration utility blocks access to the multimedia features and functions.

In a voice-only solution that uses Agent Desktop, use the CCMM Administration utility to configure Agent Desktop features and functions.

In a SIP-enabled voice contact center solution, agents must use Agent Desktop to log on and handle customer calls. Therefore, each SIP-enabled voice solution, which uses Voice Contact Server, also requires one Multimedia Contact Server.

In an Avaya Communication Server 1000 AML-based voice-only solution, where agents use Agent Desktop to log on and handle customer calls, each Voice Contact Server requires one Multimedia Contact Server. In an Avaya Communication Server 1000 AML-based voice-only solution, where agents do not use Agent Desktop but log on to their desk phones and handle customer calls, the Voice Contact Server does not require a Multimedia Contact Server.

To enable the multimedia features in the CCMM Administration utility, obtain and install a multimedia-enabled Avaya Aura® Contact Center license. Once you have obtained a multimedia license, install the new license file on the server, and reconfigure the Contact Center Manager Server server and license settings. You must also refresh all the servers in Contact Center Manager Administration. Once you have installed a multimedia-enabled license, the system enables all the multimedia features and functions.

Administrators can use the CCMM Administration utility to configure only the following, in a voice-only solution:

- Voice handling
- Customer history and web stats
- Peer to Peer IM (for SIP-enabled contact centers only)
- Screen Pops for voice contacts
- Phonebook

CCMM Administration in a voice-only solution displays only the **General Administration** and **Agent Desktop Configuration** tabs.

On the **General Administration** tab only the following options are available:

- **Server Settings**

  Note:

  You cannot add multimedia servers.

- **General Settings**

On the **Agent Desktop Configuration** tab only the following options are available:

- **General Settings**

- **Basic Screenpops**
- **Advanced Screenpops**
- **Shortcut Keys**
- **User Settings**

Administrators can configure the following using the CCMM Administration Utility:

- Starting the CCMM Administration utility on page 224
- Configuring general settings on page 225
- Configuring a Geographic Alternative Communication Control Toolkit server on page 235
- Deleting a Geographic Alternate Communication Control Toolkit server on page 236
- Configuring a Phonebook LDAP server on page 238
- Configuring Agent Desktop behavior on page 370
- Configuring the state of the Agent terminal on log off on page 371
- Configuring hotdesking on page 371
- Configuring hotdesking in a Citrix environment on page 372
- Configuring Web reporting on page 373
- Configuring Basic Screen Pops on page 376
- Configuring Advanced screen pop applications on page 380
- Configuring Advanced screen pop filters on page 381
- Configuring Advanced Screen pops on page 382
- Enabling Customer History on Voice Contacts on page 385
- Configuring Advanced Settings in a voice-only solution on page 391
- Configuring User Settings in a voice-only solution on page 408

Chapter 23: General configuration

The Contact Center Multimedia server supports multimedia contacts. To manage the multimedia contacts, you must configure general administrator settings and global routing options.

Prerequisites for general configuration

Procedure

Log on to the Contact Center Manager Administration application. See *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.

Starting the CCMM Administration utility

Before you begin

- Configure Internet Explorer.

About this task

Use the CCMM Administration utility to commission and maintain multimedia resources. To start the CCMM Administration utility, you must first log on to Contact Center Manager Administration.

Procedure

1. Start Internet Explorer.
2. In the Address box, type the URL of the Contact Center server. For example, type `https://<server name>`, OR if you turned off Web Services security, type `http://<server name>`, where *<server name>* is the computer name of the Contact Center server.
3. Press **Enter**.
4. In the main logon window, in the **User ID** box, type an administrator user name.
5. In the **Password** box, type the password.
6. Click **Log In**.

7. On the Launchpad, click **Multimedia**.
8. In the left pane, select the CCMM server to administer.

   The system displays the Multimedia Administration screen in the right pane.
9. Select **Install prerequisite software**.
10. Click **Launch Multimedia Client**.
11. On the **File Download** box, click **Run**.

    Important:

    If you see an **Application Run Security Warning** or a **SmartScreen Filter** warning message, confirm the **Publisher** is Avaya or that you are launching from a trusted link, before continuing to run the utility.

    The prerequisite software takes some time to install. After the install, the CCMM Administration utility appears.

Configuring general settings

About this task

Configure the system license for the Contact Center Multimedia server. The license you choose must match the system license purchased for your contact center. Choose from Nodal or Corporate licensing. Nodal licensing is for single sites of Contact Center; corporate licensing enables multiple sites.

You can also configure the RTD Multicast settings for Contact Center.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **General Administration**.
3. Click **General Settings**.
4. Under **License Type**, select the type of license used in your contact center.
5. Under **RTD Multicast Configuration**, in the **Multicast IP** box, type the Multicast send IP address from Contact Center Manager Server.
6. Under **RTD Multicast Configuration**, in the **Port** box, type the skillset port number from Contact Center Manager Server.
7. Click **Save**.

Configuring the reporting credentials

About this task

Configure the password for the mmReport user. The mmReport user is configured in the Multimedia database to pass data and reporting information to Contact Center Manager Administration to generate real-time and historical reports, and integrated reporting.

If you change the password in the Contact Center Multimedia Administrator application, you must update the Contact Center Multimedia password in Contact Center Manager Administration.

Note:

In a voice-only solution, you cannot set a password for the mmReport user.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **General Administration**.
3. Click **General Settings**.
4. In the Reporting Credentials section, under **Reporting Account Password Reset**, select the account ID for the reporting. The default account is mmReport.
5. Click **Set Password** to use the default password. The default password is assigned to new agents.

   OR

   Type the new password in the **New Password** and **Confirm Password** boxes.

   The password must fulfill the following complexity criteria:

   - Must be between 8 to 20 characters
   - Must contain a number
   - Must contain at least one uppercase letter and at least one lowercase letter
   - Must not contain spaces
   - Must not contain any of these characters: \ & : < > |
6. Click **Save**.

Adding administrators

About this task

Add administrators for the Contact Center Multimedia server to control access to configuration components in your contact center. For example, one administrator account can provide access to configure Web services.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **General Administration**.
3. Click **Administrator Settings**.
4. Click **New**.
5. In the **General identification** section, type the last name, the first name, and the user name of the Administrator.
6. In the **Contact Details** section, add information about how to contact the Administrator, such as the phone number, fax number, and email address.
7. In the **Password** section type and confirm your password.

   The password must fulfill the following complexity criteria:

   - Must be between 8 to 20 characters
   - Must contain a number
   - Must contain at least one uppercase letter and at least one lowercase letter
   - Must not contain spaces
   - Must not contain any of these characters: \ & : < > |
8. Optional: Select the **Allow Administrator to login externally via Web Services** check box.

   Using **Allow Administrator to login externally via Web Services**, a specific administrator level account can call on Web services and get unlimited access to Avaya Aura® Contact Center data and services not directly owned by this user. This supports custom client developed web service dependent applications, which need privileged access to the Avaya Aura® Contact Center Multimedia database.

   Therefore, users can get external access to services in the Avaya Aura® Contact Center system, from within client internal networks only.

   Warning:

   You must never activate **Allow Administrator to login externally via Web Services** on an external facing system. You must use it within the organizational internal networks only.

   You cannot add web service support to the predefined accounts that ship with the system for security reasons. You must create a new account to get external access to the web services.

9. Click **Save**.

Removing administrators

About this task

Remove an administrator account that you no longer require in your contact center.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **General Administration**.
3. Click **Administrator Settings**.
4. Select the administrator account to remove.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the decision.

Configuring office hours

Before you begin

- Know the office hours of the contact center.

About this task

Configure the days and hours that your contact center is open each week.

Configuring the office hours is important to determine accurate queued time for contacts that can have a delayed response such as email, voice mail, SMS, scanned documents, and faxes. For example, if a contact is received on Friday and processed on Monday and you configure the office hours to show the contact center is closed over the weekend, the queue time for the contact only includes the time the contact center is open.

You can use the office hour calendar in email rules to determine the skillset to which to route the contact. The email rules can send a specific response if the office is closed.

The office hour calendar uses sliders to indicate closed times for your contact center. The Start Closed Period slider is a blue triangle (). The End Closed Period slider is a red triangle (). Each

closed period is shown in red with a Start Closed Period and End Closed Period at the beginning and end of the closed office hours.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **General Administration**.
3. Click **Office hours**.
4. Under **Template**, type the name of a calendar to configure.
5. Configure holidays for the office hour template.
6. Beside a day of the week, click .
7. For the day you select, move the Start Closed Period  and End Closed Period  sliders to define a period when the contact center is closed.

   Open hours for the contact center are shown by the green bars. Closed hours are in red.
8. Repeat step 6 on page 229 and step 7 on page 229 for every day of the week.
9. Click **Save**.

Configuring holidays

Before you begin

- Identify the closed days of the contact center.

About this task

Configure the days and times that your contact center is open for holidays.

Configuring the office hours is important to determine accurate service levels for contacts that can have a delayed response such as email, voice mail, SMS, scanned documents, and faxes. For example, if a contact is received on a holiday, the queue time for the contact includes only the time the contact center is open.

You can use the office hour calendar in email rules to determine the skillset to which to route the contact.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **General Administration**.
3. Click **Office hours**.
4. Under **Template**, type the name of a calendar to configure.
5. In the holiday box, under **Name**, type the name of a public holiday.
6. Select the **Holiday Date** for the holiday and specify the time for the holiday. You can choose from **All Day** or a specify **Start time** and **End time**.
7. Click **Save**.

Applying office hours

Before you begin

- Create a calendar template with office hours or holidays. See Configuring office hours on page 228 or Configuring holidays on page 229.

About this task

Apply a designated calendar showing open and closed hours of the contact center controlled by the Contact Center Multimedia server.

The designated calendar is used in email settings for the contact center.

You can respond to email messages by selecting the office hours calendar to send automatic messages to incoming email contacts. You can select which rule group to apply the global office hours to. For more information, see Creating or changing rules on page 265.

You can also configure a calendar for each skillset in your contact center. For more information about configuring office hours for a skillset, see Configuring skillsets for email on page 247.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. In the left pane, click **General Settings**.
4. Under **Office Hours**, select the **Out of office hours treatment is enabled** check box to automatically send an out-of-office type message to the customer when the contact center is closed.

5. Select the calendar you want to use to determine the business hours for your contact center.
6. Select the automatic response for the out of office hours notice.
7. Click **Save**.

Viewing real-time traffic reports by contact

About this task

For email, voice mail, fax, SMS, and scanned documents, you can view traffic reports for each contact type.

The reports appear in the Contact Center Multimedia Administration utility to show the current traffic status. The following reports appear when you select View Reports in the left column of the Contact Center Multimedia application. You can choose the report date and the skillsets represented in all displayed real-time reports.

- The New Vs. Closed report shows the number of contacts in a new and closed state against the time for the selected date and skillsets.
- The Progress report shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for that date.
- The Closed Contacts Queue Time report shows the average time a contact spends in queue while the contact center is open.

You can change the time for the displayed traffic reports. See Configuring the displayed date for traffic reports on page 232.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select a media type that supports the traffic report views (**Text Messaging (SMS)**, **E-mail**, **Fax**, **Scanned Documents**, and **Voice Mail**).
3. Click **View Reports**.

Configuring the displayed date for traffic reports

About this task

For email, voice mail, fax, SMS, and scanned documents, you can view traffic reports for each contact type.

You can choose a date and specify the skillsets for each media type for the current reports.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. Select a media type that supports the traffic report views (**Text Messaging (SMS)**, **E-mail**, **Fax**, **Scanned Documents**, and **Voice Mail**).
3. Click **View Reports**.
4. In the bottom left corner of the report view, in the **Report Date** list, select the date for which to view the traffic for your contact center.
5. To display all skillsets, select the **Select All Skillsets** check box.

   OR

   Specify the skillsets to view. The skillsets must be valid for the contact type you review.
6. Click **Update**.

Configuring Web On Hold comfort groups for a Web communications skillset

Before you begin

- Set up the Web On Hold comfort group.

About this task

You must configure a Web On Hold comfort group on a Web communications skillset to automatically send messages to the customer's desktop. These messages are sent to the customer while they wait for an agent to respond, for a specified period of time to their initial contact, on a Web communication skillset.

For more information on Web On Hold comfort groups, see Creating Web On Hold comfort groups on page 356.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. In the **Skillset Settings** dialog box, select the skillset for which to assign a Web On Hold comfort group. The skillset must have the prefix WC for Web communications.
5. Under the **Edit Skillset** dialog box, in the **On Hold Group** list, select the group to assign to the Web communications skillset.
6. Click **Save**.

Removing a Web On Hold comfort group for a Web communications skillset

Before you begin

- The Web On Hold comfort group must be associated with the Web communications skillset.

About this task

You can remove a Web On Hold comfort group from a Web communications skillset, if the group has been deleted or if you do not want to use a specific Web On Hold comfort group.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. Under the **Edit Skillset** dialog box, in the **On Hold Group** list, select the group that you want to remove and click **Unlink Group**.
5. When the warning message asking you to confirm unlinking the Web On Hold comfort group appears, click **Yes**.

Configuring Web communications comfort groups for a Web communications skillset

Before you begin

- Set up the Web On Hold comfort group.

About this task

You must configure a Web communications comfort group on a Web communications skillset to automatically send messages to the customer's desktop. These messages are sent to the customer while they wait for an agent to respond, for a specified period of time, either to their initial contact, or during the communication, on a Web Communications skillset.

For more information on Web communications comfort groups, see Creating Web communications comfort groups on page 358.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. In the **Skillset Settings** dialog box, select the skillset for which to assign a Web communications comfort group. The skillset must have the prefix WC for Web communications.
5. Under the **Edit Skillset** dialog box, in the **Comfort Group** list, select the group to assign to the Web communications skillset.
6. Click **Save**.

Removing a Web communications comfort group from a Web communications skillset

Before you begin

- The Web communications comfort group must be associated with the Web communications skillset.

About this task

You can remove a Web communications comfort group from a Web communications skillset, if the group has been deleted or if you do not want to use a specific Web communications comfort group.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. Under the **Edit Skillset** dialog box, in the **Comfort Group** list, select the group that you want to remove and click **Unlink Group**.
5. When the warning message asking you to confirm unlinking the Web communications comfort group appears, click **Yes**.

Configuring a Geographic Alternative Communication Control Toolkit server

About this task

Avaya Aura® Contact Center supports High Availability and geographic disaster recovery and data resiliency. You can configure a geographic alternate CCT server to achieve High Availability for your contact center.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **General Administration**.
3. Click **Server Settings**.
4. Click **New**.
5. In the **Server Type** list, select the **Geographic Standby CCT Server** option.
6. In the **Hostname** box, type the name of the CCT server.
7. In the **Port Number** box, type the port number of the CCT server.

   The default port number for the CCT server is 29373.
8. Click **Save**.

Deleting a Geographic Alternate Communication Control Toolkit server

Before you begin

- Ensure that the CCT server is not in use.

About this task

You can delete a geographic alternate CCT server if you no longer use that server.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **General Administration**.
3. Select the **Geographic Standby CCT Server** that you want to delete.
4. Click **Delete**.

   The system displays a Warning dialog box.
5. Click **Yes** to confirm the decision.

Configuring a Reporting Server

About this task

Configure a reporting server for peer-to-peer Instant Messaging and voice history.

Procedure

1. Open the Multimedia Administration utility.
2. In the left pane, select **General Administration**.
3. Click **Server Settings**.
4. Select **Reporting Server (P2P IMs and Voice history)**.
5. Click **Edit**.
6. In the **Server Name** box, type the name of the Contact Center Voice Contact Server.
7. In the **Server Port** box, type the port number. The default port number is 7081.
8. Click **Save**.

Configuring a Directory LDAP server

About this task

The Lightweight Directory Access Protocol (LDAP) server contains databases of customer addresses and other information to use when handling email contacts in the Agent Desktop. Agents can select recipients from the Directory LDAP list when composing an email message.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **General Administration**.
3. Click **Server Settings**.
4. Select the **Directory LDAP Server**.
5. Click **Edit**.
6. Select **Anonymous Logon** to enable the administrator to log on to the LDAP server without having to supply a username or domain.
7. Select **Enable Address Book Retrieval** to enable the directory lookup.
8. In the **User** field, type the user name for the administrator on the LDAP server in the format domain name\user name.
9. In the **Password** field, type the password for the administrator on the LDAP server.
10. In the **Polling Interval** field, type the polling interval, in hours, for the interval between polls for the email server lookup.
11. In the **Search Base** field, specify the preciseness of the LDAP search. For example, in a large enterprise of tens of thousands of people, it is not advisable to search for all users. In such a case, use a more restrictive search base, such as search for names in the local workgroup.
12. Click **Edit Server** to change the properties of the Directory LDAP server.
13. In the **Server Name** field, type the server name for the email server that you use to get email addresses. The default port number for the LDAP server is 389.
14. In the **Server Port** box, type the port number for the server.
15. Select **Use TLS** if you want Agent Desktop to communicate securely with the Directory LDAP server. The server specified must support TLS.
16. Click **Save**.
17. Click **Test** to test the connection to the LDAP server.

18. Click **Save**.

Configuring a Phonebook LDAP server

Before you begin

- Configure the Directory LDAP server. See Configuring an LDAP server on page 237.

  Important:

  To retrieve contacts from the LDAP server, ensure you select the **Enable Address Book Retrieval** check box.

- Ensure that the Contact Center LDAP Phone Book check box on the Multimedia, Agent Desktop Configuration, and Advanced Settings page is enabled.

About this task

Configuring a Phonebook LDAP server provides agents with a list of contacts during a voice call or while working on an email contact.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Agent Desktop Configuration**.
3. On the Agent Desktop General Settings screen, click **Advanced**.
4. On the Advanced Settings screen, enable **Contact Center LDAP Phone Book**.
5. Click **Save**.
6. Click **Yes**.
7. Click **OK**.
8. In the left pane, select **General Administration**.
9. Click **Server Settings**.
10. Click **New**.
11. In the **Server Type** list, select the **Phonebook LDAP Server** option.
12. In the **User** field, type the user name for the administrator on the Phonebook LDAP server in the format domain name\user name.
13. In the **Password** field, type the password for the administrator on the Phonebook LDAP server.
14. In the **Polling Interval** box, type the polling interval, in hours, for the interval between polls for the email server lookup.
15. In the **Search Base** field, specify the precision of the Phonebook LDAP search.

For example, in a large enterprise of tens of thousands of people, it is not advisable to search for all users. In such a case, use a more restrictive search base, such as search for names in the local workgroup.

16. Click **Edit Server** to change the properties of the Phonebook LDAP server.
17. In the **Server Name** box, type the server name.
18. In the **Server Port** box, type the port number for the server.
19. Select **Use TLS** if you want Agent Desktop to communicate securely with the Phonebook LDAP server. The server specified must support TLS.
20. Click **Save**.
21. Click **Test** to test the user name, password, and search base, by connecting to the configured server to retrieve contacts.
22. Click **Save**.

Chapter 24: Outbound configuration

To create, monitor, and add data to an outbound campaign, use the Outbound Campaign Management Tool.

You must use the Multimedia Administration tool to configure how contacts are routed to a contact type using a skillset. Complete all other configuration for previewed outbound campaigns in the Outbound Configuration Management Tool. For more information, see *Avaya Aura® Contact Center Client Administration*.

Note:

Outbound configuration procedures do not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Prerequisites for Outbound configuration

Procedure

- Ensure that you are licensed for Outbound contacts in your contact center.
- Ensure that the Moving Window Skillset Multicast Rate is five seconds or greater. Configure the Moving Window Skillset Multicast Rate using the CCMS Multicast Address and Port Configuration tool.
- Ensure that the route points (CDN) are configured in Contact Center Manager Administration.

Configuring a route point for an Outbound skillset

About this task

Configure a route point for an outbound skillset to route outbound contacts to a particular direction. Skillsets are used to assign the contacts to agents.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **General Administration**.

3. Click **Skillset Settings**.
4. In the **Skillset Settings** dialog box, select the skillset for which to assign a route point.

   The skillset must have the prefix OB for outbound.
5. Under the **Edit Skillset** dialog box, in the **Route Point** list, select the route point to assign to the outbound skillset.
6. Click **Save**.

Variable definitions

Name	Description
Route point	A location in the open queue that enables incoming contacts to queue and run through a script on the Contact Center Manager Server.

Chapter 25: Email configuration

This chapter describes how to set up your contact center with the optional configurations for routing email contacts to fulfill your customer requirements.

When you commission your contact center, you configure the email server, a default email skillset, and a default recipient with at least one rule group. The default settings ensure email messages go only to an agent with the ability to handle email messages. You can customize your contact center with additional skillsets, rule groups and email servers.

To further enhance your customer service, you can configure routing tools to use in rule groups. Use keyword groups and sender groups to decide how to route contacts. Configure which skillset and priority the email contact is assigned to based on the input for routing contacts. Use automatic suggestions for the agent to reply quickly to an email or automatic responses to send a reply to the customer without agent interaction. You can close the contact immediately after the automatic response. This chapter describes how to configure all optional routing tools.

You can configure outbound email settings, such as which skillset to use as a reply address and a list of email addresses that must not receive automatic responses. For each skillset you use to route contacts, you can have a signature with your corporate branding or special information based on the skillset.

Other types of contacts generate email messages that are routed using the inbound and outbound email options.

Reports appear in the Contact Center Multimedia Administration utility to show the current status of the email traffic. The following reports appear when you select email and View Reports in the left column of the Contact Center Multimedia application. You can choose the report date and the skillsets represented in all displayed real-time reports.

- Email (New Vs. Closed) shows the number of contacts in a new and closed state against the time for the selected date and skillsets.
- Email Progress shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for that date.
- Email Closed Contacts Queue Time shows the average time an email contact spends in queue while the contact center is open.

You can configure general email settings to minimize space and format special characters for other languages.

Note:

Email configuration procedures do not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Prerequisites for email configuration

Procedure

Ensure that you are licensed for email contacts.

Configuring the email server names

About this task

Configure the email server names to identify the inbound server (POP3 or IMAP) for email messages received by the contact center and the outbound server (SMTP) for email messages sent by the contact center.

If you configured the email servers during installation and the names of the inbound and outbound email servers remain unchanged, you can skip this procedure.

You can configure secondary inbound and outbound email servers. If a primary email server fails, the email retrieved during the failure is duplicated in the Multimedia database when you restore the primary server.

Avaya recommends that you use POP3 as the inbound protocol to receive email messages.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **General Administration**.
3. Click **Server Settings**.
4. Under Edit Current Servers select **Inbound Mail Server**.
5. Click **Edit**.
6. In the **Primary Hostname** field, type the name of the server that receives email messages.
7. In the **Inbound Protocol** field, select the protocol that is used for receiving email messages. You can choose one of the following:
   - **IMAP**
   - **POP3**

8. In the **Encryption** field, select the security protocol that is used for receiving email messages. You can choose one of the following:
   - **Clear Text** (Default)
   - **TLS**
   - **STARTTLS**
9. In the **Port Number** field, type the port number for the email server.
10. If you have a backup email server, in the **Secondary Hostname** field, provide a host name for the backup server.
11. Click **Save**.
12. Under Edit Current Servers, select **Outbound SMTP Server**.
13. Click **Edit**.
14. In the **Primary Hostname** field, type the name of the server that sends email messages.
15. In the **SMTP Authentication** field, select the SMTP authentication, if required, for your outbound email server.
16. In the **Encryption** field, select the security protocol that is used for sending email messages. You can choose one of the following:
    - **Clear Text** (Default)
    - **TLS**
    - **STARTTLS**
17. In the **Port Number** field, type the port number for the email server.
18. If you have a backup email server, in the **Secondary Hostname** field, provide a host name for the backup server.
19. Click **Save**.

Variable definitions

Name	Description
Port Number	Port number for the email server.
Primary Hostname	The name of the server that receives email messages.
Secondary Hostname	Name of a secondary email server, if one is available in your contact center.

Adding an email server

About this task

Add or update the email server for your Contact Center Multimedia server so you can poll multiple email servers in your contact center for email messages to be routed. You can retrieve email messages for the contact center only if you are licensed to use the email feature.

If you select TLS or STARTTLS as the encryption type for incoming or outgoing mail, you must add a valid certificate on the Contact Center Multimedia server. For more information, see Adding a certificate for use with TLS email connections on page 279.

Avaya recommends that you use POP3 as the inbound protocol to receive email messages.

Important:

Contact Center Multimedia supports adding a maximum of five POP3 or IMAP servers as inbound email servers and five SMTP servers as outbound email servers. You can have a mix of email servers that have POP3 or IMAP protocols for receiving email messages and SMTP protocol for sending email message with a mix of TLS, STARTTLS, and no security channels.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **General Administration**.
3. Click **Server Settings**.
4. Under Edit Current Servers, click **New**.
5. Select **Inbound Mail Server** to add a new inbound email server.
6. In the **Primary Hostname** field, type the name of the server that receives email messages.
7. In the **Inbound Protocol** field, select the protocol that is used for receiving email messages. You can choose one of the following:
   - **IMAP**
   - **POP3**
8. In the **Encryption** field, select the security protocol that is used for receiving email messages. You can choose one of the following:
   - **Clear Text** (Default)
   - **TLS**
   - **STARTTLS**
9. In the **Port Number** field, type the port number for the email server.
10. If you have a backup email server, in the **Secondary Hostname** field, provide a host name for the backup server.
11. Click **Save**.

12. Under Edit Current Servers, click **New**.
13. Select **Outbound SMTP Server** to add a new outbound email server.
14. Click **Edit**.
15. In the **Primary Hostname** field, type the name of the server that sends email messages.
16. In the **SMTP Authentication** field, select the SMTP authentication, if required, for your outbound email server.
17. In the **Encryption** field, select the security protocol that is used for sending email messages. You can choose one of the following:
    - **Clear Text** (Default)
    - **TLS**
    - **STARTTLS**
18. In the **Port Number** field, type the port number for the email server.
19. If you have a backup email server, in the **Secondary Hostname** field, provide a host name for the backup server.
20. Click **Save**.

Deleting an email server

About this task

Delete an email server or other nonessential server if the server is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **General Administration**.
3. Click **Server Settings**.
4. Select the sever to delete.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Configuring skillsets for email

Before you begin

- If required, configure an office hour template. See Configuring office hours on page 228 and Configuring holidays on page 229.

About this task

Configure a route point for each skillset, to use the skillsets in rules. A route point is a location on the open queue that enables incoming calls to be queued and run through a script on the Contact Center Manager Server.

An automatic signature is text automatically added at the bottom of an outgoing message. For example, you can encourage customers to visit your customer support website by adding the URL and other promotional information to every message. You can also use the automatic signature to add disclaimer text to messages.

You can also apply an office hours template for your skillset. If agents in a different time zone or different department have a different set of office hours, you can apply an office hour template that is different from the global office hours schedule configured in general email settings to this skillset.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **General Administration**.
3. Click **Skillset Settings**.
4. Select a skillset for which to assign a route point.
5. Click **Edit**.
6. From the **Route Point** list, select the route point to assign to the skillset.
7. Under **Office Hours**, choose an office hour template that gives the office hours particular to the selected skillset.
8. If applicable, in the **Auto Signature** box, type the signature to assign to the skillset.
9. Click **Save**.

Creating or changing a recipient mailbox

Before you begin

- Ensure that any enabled email address you want to configure in the Email Manager is already configured on your corporate email server.

About this task

Create a recipient email box to ensure that at least one email box is configured for your contact center. You must configure one recipient to commission the server. You can create additional mailboxes to have the Contact Center Manager Server poll a mailbox on the email server and handle contacts based on the recipient address.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Recipient Addresses**.
4. Click **New**.

   OR

   Select a recipient address, and click **Edit**.
5. If you select **New**, select **Mail Store** from the **Mailbox Type** list.
6. Under Mailbox Details, in the **Mailbox** box, type the SMTP mailbox name.
7. In the **Domain** field, type the domain for your email server.
8. In the **Display Name** field, type the name to appear in the email From address.
9. In the **Password** field, type the password for the mailbox.

   Important:

   When you change a password on the email server, you must update this password in the Multimedia Administration Tool.
10. In the **Confirm Password** field, type the same password you typed in the Password box.
11. In the **Inbound (POP3) Server** field, select the host name of your POP3 or IMAP server along with the respective security protocol.
12. In the **Inbound Mail Threshold** field, type the maximum number of email messages to be retrieved from the mailbox every scan interval.

    You can enter a different value for this variable for each mailbox.
13. In the **Outbound SMTP Server** field, select the host name of your SMTP server.
14. In the **Rule Group** field, select the name of the Rule Group to assign to the recipient mailbox.
15. Click **Save**.

Variable definitions

Name	Description
Display Name	The name to appear in the email From address. For example, Sales Department.
Domain	The domain name for the email server.
Mailbox	The name of a mailbox on the email server. If the Contact Center Multimedia server is in the same domain as the email server, in the Mailbox Name box, type the address, and in the E-mail Domain box, type the domain name. If the Contact Center Multimedia server is not in the same domain as the email server, and you are using Windows 2000, in the Mailbox Name box, type the address in the format domain\user. If the Contact Center Multimedia server is not in the same domain as the email server, and you use a version of Windows later than Windows 2000, in the Mailbox Name box, type the address in the format user@domain. **Important:** Mailbox names are case-sensitive. You must type the mailbox name exactly as it appears on your server.
Username	The username used to access the mailbox on the email server.
Password and Confirm	The password used to access the mailbox on the email server. Type the password in the Confirm box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.
Inbound Mail Threshold	The maximum number of email messages to be retrieved from the mailbox every scan interval. You can enter a different value for this variable for each mailbox. The default value is 10.
Rule Group	The name of the rule group that applies to this recipient mailbox. Configure rule group properties in the Contact Center Multimedia Administrator.

Table continues…

Name	Description
Inbound (POP3 or IMAP) Server	The name of the email server, either POP3 or IMAP, that handles email messages coming into the contact center.
Outbound (SMTP) Server	The name of the email server that delivers email messages that leave the contact center.

Creating or changing an alias for a recipient mailbox

Before you begin

- Ensure that any enabled email address you want to configure in the Email Manager is already configured on your corporate email server.
- Configure a mail store recipient mailbox. See Creating or changing a recipient mailbox on page 247.

About this task

Create an alias, or another name, for the recipient email box.

For example, the mailbox general@magscripts.com can have the aliases carz@magsubscriptions.com and planez@magsubscriptions.com. Email messages addressed to either alias are forwarded to the general@magscripts.com mailbox. The Email Manager routes the email messages according to the alias-based rules.

Aliases can be useful to filter email messages. For example, you can define an alias for a short promotional period after which email messages that arrive at that alias are discarded.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Recipient Addresses**.
4. Click **New**.

   OR

   Select the alias and click **Edit**.
5. In the **Mailbox Type** list, select **Alias**.
6. Under **Mailbox Details**, in the **Mailbox** box, type the SMTP mailbox name.
7. In the **Domain** box, type the domain for your email server.
8. In the **Display Name** box, type the name of the alias set up on the email server.
9. In the **Rule Group** box, select the name of the Rule Group to assign to the alias for the recipient mailbox.

10. In the **Outbound SMTP Server** box, ensure that the host name of your SMTP server appears.
11. Select the **Use alternative username for SMTP Authentication** check box if you configure an inbox as an alias.

    If SMTP authentication is enabled on your email server, and you use aliases, log on to the SMTP server with a different user name.
12. In the **Username** box, type the username of the mail store recipient address.
13. In the **Password** box, type the password of the mail store recipient address.

    Important:

    When you change a password of the mail store recipient address on the email server, you must update this password in the Multimedia Administration Tool.
14. In the **Confirm Password** box, type the same password you typed in the Password box.
15. Click **Save**.

Variable definitions

Name	Description
Alias	An alias is an address that forwards all email messages it receives to another email account.
Display Name	The name to appear in the email From address. For example, Sales Department.
Domain	The domain name for the email server.
Mailbox	The name of a mailbox on the email server. If the Contact Center Multimedia server is in the same domain as the email server, in the Mailbox Name box, type the address, and in the E-mail Domain box, type the domain name. If the Contact Center Multimedia server is not in the same domain as the email server, and you are using Windows 2000, in the Mailbox Name box, type the address in the format domain\user. If the Contact Center Multimedia server is not in the same domain as the email server, and you use a version of Windows later than Windows 2000, in the Mailbox Name box, type the address in the format user@domain.

Table continues…

Name	Description
	Important: Mailbox names are case-sensitive. You must type the mailbox name exactly as it appears on your server.
Username	The username used to access the mailbox on the email server.
Password and Confirm	The password used to access the mailbox on the email server. Type the password in the Confirm box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.
Rule Group	The name of the rule group that applies to this recipient mailbox. Configure rule group properties in Contact Center Multimedia Administrator.
Outbound (SMTP) Server	The name of the email server that delivers email messages that leave the contact center.

Deleting a recipient mailbox

Before you begin

- Before you delete a mailbox, you must ensure that no email messages are sent to the inbox and no aliases are directed to that mailbox.
- Avaya recommends that you archive all contacts associated with a recipient before you delete the recipient.

About this task

Delete a recipient mailbox from your system if you no longer require it to monitor email. Removing extra mailboxes saves space in your database.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Recipient Addresses**.
4. Select the address from the recipient list that you want to delete.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion of the recipient mailbox.

Updating the system default rule

Before you begin

- Ensure that you know the default settings for the system delivery failure rule:
  - use the email default skillset, EM_Default_Skillset
  - use no automatic response
  - assign priority 3
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, EM_Default_Skillset is used.
  - If you delete EM_Default_Skillset, the system stops processing email messages.
- Configure the route points for the skillset you assign to the system default rule. For more information, see Configuring skillsets for email on page 247.

About this task

Update the system default rule to ensure that an email arriving at each configured recipient mailbox is assigned a skillset and can be routed.

When you create a recipient mailbox, the system default rule is copied as the last regular rule into the list of rules for the recipient mailbox.

The automatic signature is text appended to each email message sent from the contact center in addition to the agent message. The text in the automatic signature contains corporate disclaimer information and must be in fixed-width font. The automatic signature appears in an email message after any personal signature, which is configured in the Agent Desktop application.

The system default rule is used in every rule group configured in Contact Center Multimedia.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **System Rules**.
4. Under **System Default Rule**, from the **Skillset** list, select a skillset name.
5. To change the automatic response settings, under **Auto Responses**, select another automatic response from the list.
6. To change the priority, under **Priority**, select a different priority for the contact.
7. Click **Save**.

Variable definitions

Name	Description
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager Server database. You must select a route point for a skillset used to route contacts.
Auto Response	A message sent to a customer with no agent interaction. An automatic response can be an intelligent response, such as a sales promotion flyer, or an acknowledgement, such as, “Thank you for your email. We will respond to you within three days.”
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 10. For example, a call with priority 1 is handled before a call with priority 10.

Updating the system delivery failure rule

Before you begin

- Ensure that you are licensed to handle email messages.
- Ensure that you know the default settings for the system delivery failure rule:
  - use the email default skillset, EM_Default _Skillset
  - use keyword group delivery failure keywords
  - assign priority 10 (lowest)
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, EM_Default_Skillset is used.
  - If you delete EM_Default_Skillset, the system stops processing email messages.
- Configure the route point for the skillset you plan to assign to the system delivery failure rule. See Configuring skillsets for email on page 247.

About this task

Update the system delivery failure rule to ensure that any email message that contains particular phrases such as undeliverable, returned mail, unknown recipient, delivery failure, or delivery report is deleted and not assigned to an agent.

When you create a recipient mailbox, the system delivery failure rule is copied as the first regular rule into the list of rules for the recipient mailbox.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **System Rules**.
4. Under **System Delivery Failure** Rule, from the **Skillset** list, select a skillset name.
5. To change the keyword group, under **Keyword Group**, select an existing keyword group from the list.
6. To change the priority, under **Priority**, select a different priority for the contact.
7. Select the **Will close contact** check box to have the rule to close the contact.
8. Click **Save**.

Variable definitions

Name	Description
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager Server database. You must select a route point for a skillset used to route outbound contacts.
Keyword group	A list of words that you can search in an email message. Keyword groups associate keywords and expressions considered important by the contact center to be handled in a particular way.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 10. For example, a call with priority 1 is handled before a call with priority 10.
Will close contact	Select the check box to close the email contact after the system delivery failure rule determines that the

Table continues…

Name	Description
	contact is not appropriate for the contact center. Clear the check box to leave the email contact open for review.

Creating or changing a keyword group

About this task

You must assign at least one keyword to a keyword group before you can save the keyword group.

The keyword search in an email message is not case-sensitive. For example, if you add the word John, the Email Manager also matches JOHN and john.

The Keyword box supports the Unicode UTF-8 character set.

You can specify a spelling accuracy in the keyword group.

Keyword groups support only asterisks (*) and question marks (?) as wildcard characters. The asterisk (*) represents multiple characters. For example, t* specifies a list of all the words that start with t. The question mark (?) represents a single character. For example, p?t specifies all three letter words that start with p and end with t.

A keyword does not support the following characters: +-!(){}[]^"~:\&&||#$@€/><,.‘;=%£&¬|`‘“. If you use any of these characters in your keywords, you receive an error message stating that the keyword contains invalid characters.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Keyword Groups**.
4. Click **New** or **Edit**.
5. Under **Keyword Group**, in the **Group Name** box, type a unique name for the keyword group.
6. In the **Keyword** box, type a word or a group of words related to the keyword group you create.
7. Optional: To allow close misspellings of the word, select the **Allow spelling inaccuracies** check box.

   The system displays the following levels of accuracy:

   - **Low (greater than 70% accuracy)**
   - **Medium (greater than 80% accuracy)**

- **High (greater than 90% accuracy)**

8. Optional: Select the required level of accuracy.
9. Click **>**.

   The keyword or expression is added to the list, and the keyword group is created.
10. Repeat step 6 on page 256 through step 9 on page 257 to add more keywords to the list.
11. Click **Save**.

Variable definitions

Name	Description
Name	Name of the keyword group. The name must be unique and less than 64 characters.
Keyword	A word, or string of characters, used to search the email message for particular text to determine the routing of the contact. A maximum of 50 keywords can be in each keyword group.
Allow spelling inaccuracies	Select the check box to allow small inaccuracies in spelling of words. Specify to allow a spelling inaccuracy of 70%, 80%, or 90% in the keyword list. For example, to allow charles, charlie, and charley in the search for the keyword charlie, you can select a low (70%) degree of accuracy because 2 of the 7 characters or 71% of the characters are correct. Inaccuracies of 80% or 90% do not allow the error.

Deleting a keyword from a keyword group

About this task

Remove a keyword from a keyword group. The remaining keywords and phrases in the keyword group remain active for rules.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Keyword Groups**.
4. Select a keyword group from the **Keyword Groups** list.

5. Click **Edit**.
6. In the **Keywords in Group** list, select the keyword.
7. Click **Remove**.

   The system displays a Warning dialog box.
8. Click **Yes** to confirm the deletion.
9. Click **Save**.

Deleting a keyword group

About this task

Delete a keyword group. After you remove the keyword group, you cannot use it in any rule. In certain scenarios, rules that use the deleted keyword group do not route the contact as expected.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Keyword Groups**.
4. Select a keyword group from the **Keyword Groups** list.
5. Click **Delete**.
6. Click **Delete**.

   The system displays a Warning dialog box.
7. Click **Yes** to confirm the deletion.

Creating or changing prepared responses

About this task

There are three types of prepared responses; auto response, chat history header, and auto suggestion.

You can use automatic responses to automatically send responses to a sender without agent intervention. Chat history headers provide email headers for sending chat history to a customer. Suggested responses give agents template text for common responses, which they can review and edit and send as a response. The body of a prepared response is limited to 3900 characters. This limit includes hidden characters such as HTML tags.

You must add a suggested response to a rule group, to make it available to agents on Agent Desktop. To send prepared chat history headers, you must configure a header on each WC skillset.

Prepared responses support both standard and inline attachments. You can add inline attachments such as company logos to the responses. You can include only images as inline attachments. The formats supported are .gif, .bmp, .jpg, and .png.

Agents can also place inline attachments (only as images) in email messages.

Inline attachments display complete information within the body of the email. This makes the information easily accessible to customers, even without explicitly opening the attachment. For example, adding a company logo, as an inline image, increases brand awareness.

Examples of prepared responses include the following:

- provide the customer with their Web logon ID and password (password reminder automatic response)
- inform a customer if your office is closed (out-of-office automatic response)
- acknowledge the receipt of an email contact (automatic response, or an automatic acknowledgement)
- include standard content on a web chat history email
- provide specific information in response to rule inputs (suggested response)

Configuring prepared responses for a rule is optional.

You can create categories for the prepared responses. The categories enhance the ability of the agent to search through the prepared responses on Agent Desktop.

A password reminder and an out-of-hours automatic response are configured by default. You cannot delete the default automatic responses.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Prepared Responses**.
4. In the **Prepared Responses** table, click **New Response**.

   OR

   In the **Prepared Responses** table, select a response, for editing that particular prepared response.
5. In the **Name** box, type or edit the name of the prepared response.
6. In the **Type** box, select the type of response.
7. In the **Subject** box, type or edit the subject of the response email message.
8. In the **Body** box, type or edit the message to include in the response.

   Use the formatting bar described below to apply formats to your email message.

9. **(Optional)** Click the **Image** icon to add images or inline images to the response.

   The system displays the Insert Image dialog box.

10. **(Optional)** Beside the **Attachment** box, click **Add** to add attachments to the response.

    The system displays the Attachment dialog box.

11. **(Optional)** Choose a category for the prepared response to make it easier for agents to navigate on Agent Desktop.
12. Click **Save**.

Variable definitions

Name	Description
Name	The name of the automatic response. The name must be unique.
Type	The type of prepared response. Auto-Response is a reply that Contact Center Multimedia can send automatically when it receives an email message. Chat History Header provides common headers for Web Chat history emails. You must configure this response on each WC skillset for which you want to use this response. Auto-Suggest is a template that agents can use to provide common responses to customers. You must add a suggested response to a rule group, to make it available to agents.
Subject	The subject of the prepared response used as an email message.
Body	The body of the prepared response. The body is limited to 3900 characters. The body can include attachments, formatting, and variables for a customer. To access the variables for the content, insert a placeholder by right-clicking the content and selecting the placeholder from the menu.
Categories	The category for the prepared response. Specifying the category makes it easier for agents to find automatic suggestions on Agent Desktop.
Attachments	The attachment is stored on the Contact Center Multimedia server for later use.
Image	Inline images are seen directly within the message body. The inline image file size limit is the same as

Table continues…

Name	Description
	the current limit set for attachments in Agent Desktop.
Browse	Available only when you select Image. Browse to locate the inline image that you want to include in the email.
Image Address (URL)	Type the url for the inline image that you want to include in the email.
Alternate text	Type the alternative text for the image. Alternate text is what the customer views if their email client cannot display the image.
Align	Select the alignment of the image. The options are inline, left, and right.
Border	Inserts a border around the image. For example, enter 2 to add a double-sized border around the image.
Margin	Inserts a margin around the image.
Insert Image	Insert the inline image.
Cancel	Exit the Inline Attachments fields.

Deleting prepared responses

About this task

Delete the prepared responses that are no longer used by agents in your contact center.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Prepared Responses**.
4. Select an existing prepared response.
5. Click **Delete Response**.
6. Click **Yes** to confirm the deletion.

Removing attachments from prepared responses

About this task

Remove attachments from a prepared response. The attachment file is stored on the Contact Center Multimedia server for later use.

To remove inline attachments, select the attachment and delete it from the body of the email.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left column, click **E-mail**.
3. Click **Prepared Responses**.
4. Select the prepared response from which you want to remove an attachment.
5. Select the attachment to delete.
6. Beside the **Attachments** box, click **Delete**.

   The system displays a Warning dialog box.
7. Click **Yes** to confirm the deletion.
8. Click **Save**.

Promoting suggested responses

About this task

You can configure prepared responses for agents in the contact center. An agent can use a suggested response during the contact. Contact Center Multimedia tracks the number of times the suggestion is used. If one suggestion is used often, it is considered a strong reply, and then you can promote the suggestion to an automatic response.

Promoting the suggested responses ensures that the customer receives a correct response because the agent checks it. The agent can make small changes to the suggestion until it is acceptable to run as an automatic response.

You can promote the suggested responses to an automatic response based on the following criteria:

- rules where the suggestion is assigned
- number of contacts in the past 30, 60, 90 or 120 days
- list of all suggestions that are used by agents
- number of times the suggestion is used
- percent of total contacts where the suggestion is applied by agents

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Auto-Suggest Promotion**.
4. Under **Rules**, select the rule for which to promote the suggestion.
5. In the **Number of Contacts in past** box, choose the length of time for which to see the contacts for the selected rule.
6. Under **Auto Suggestions**, review the list of suggested answers.
7. Select the suggestion to promote.
8. If you want to close the contacts with automatic suggestion, select the **Will Close Contacts** box.
9. Click **Promote**.

Creating or changing a sender group

About this task

You must place any sender addresses that you want to track in a sender group. You can use sender groups to route important sender email addresses to particular skillsets.

Using a sender group in a rule is optional.

Sender groups support asterisks (*) as wildcard characters when they are placed in the email address.

Avaya recommends that you have a maximum of 20 sender email addresses in one sender group.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Sender Groups**.
4. Click **New** or **Edit**.
5. In the **Name** box type a unique name of the sender group.
6. In the **Email Address** box, type an email address.
7. If you know the user is in the contact database, start typing an email address, and then click **Look up email**.

   Email addresses that match the characters appear in the list.

8. Click **Add** to insert the email address you looked up, or click **Add Freeform** to add your typed email address to the sender group.

   This text box supports unicode language.

9. Repeat step 5 on page 263 through step 8 on page 264 to add sender addresses to this sender group.
10. Click **Save**.

Variable definitions

Name	Description
Name	The unique name for the sender group. The name must be less than 64 characters.
Email Address	The email address to add to the sender group.
Addresses in Group	A list of addresses in a group that are reviewed when the system applies a sender group to a rule. You can specify only 50 addresses for each group.

Deleting a sender group

Before you begin

- You must have a sender group. See Creating or changing a sender group on page 263.

About this task

Delete a sender group from your contact center if it is not required in the contact center.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Sender Groups**.
4. Select the Sender Group you want to remove.
5. Click **Delete**.

   The system displays a Warning dialog box.

6. Click **Yes** to confirm the deletion.

Deleting a sender from a sender group

About this task

Remove a sender address from a sender group if it is no longer required. The remaining addresses in the sender group remain active for rules.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Sender Groups**.
4. Select a sender group from the list.
5. Click **Edit**.
6. Under **Addresses in Group** box, select the email address from the list.
7. Click **Remove**.

   The system displays a Warning dialog box.
8. Click **Yes** to confirm the deletion.
9. Click **Save**.

Creating or changing rules

Before you begin

- If you plan to use office hours for routing email messages, configure your office hours. See Configuring office hours on page 228.
- Configure at least one email skillset. See Configuring skillsets for email on page 247.
- Create keyword groups, if required. See Creating or changing a keyword group on page 256.
- Configure prepared responses (automatic responses or suggestions), if required for the rule. See Creating or changing prepared responses on page 258.

About this task

Create or change a rule to route your email contacts.

A rule is a mechanism for routing email contacts. In your contact center, you receive email messages from the customer, as well as other contacts that are routed using the rules including SMS, Fax, scanned documents, and voice mail.

You can create a rule with one or more of the following routing options:

- determine when the email was received (office hours)
- determine who sent the email (sender groups)

- look for specific characters, words or phrases (keywords)

Rules can send an automatic response to a customer and thus requires no interaction by an agent.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Rule Groups**.
4. Click **New** or select an existing Rule Group and click **Edit**.
5. Under **Rules**, click the plus sign (+) button.

   OR

   Select an existing rule.
6. Under **Current Search Criteria**, click **New** and choose the criterion to add to the rule.
7. Select the criterion from the **Add New Criterion** drop-down box

   You can choose between **Keyword Match** and **Sender Group**.
8. Click **Go**.
9. Configure the keyword match or sender group to use.
10. Repeat step 5 on page 266 to step 7 on page 266 to select a maximum of five criteria for the rule.
11. Click **OK**.
12. Under **Current Search Criteria**, choose the weightage for each criterion.

    The total weightage must add up to 100 percent.
13. Under **Current Search Criteria Summary**, click the blue text to view the details of each criterion you configure.
14. Click **Next**.
15. To select an automatic response for the rule, under **Available Auto-Responses**, select the configured automatic response, and then click **>**.
16. To select automatic suggestions for the rule, under **Available Auto-Suggests**, select the automatic suggestion you want to include, and then click **>**.

    To remove a suggestion, select the suggestion, and then click **<** to remove it from the rule list.
17. Click **Next**.
18. In the General Settings area, in the **Name** box, type a name for the rule.
19. In the **Priority** box, select the priority to assign to the contact.

20. In the **Skillset** box, select the skillset to apply for the rule.
21. If you want to apply the office hours to the email message, click **Will use Office hours**.
22. To close the contact, click **Will Close Contact**.
23. If you want to call an Open Interface Web service, select the **Call Open Interface web service** check box.
24. From the **Web Service** drop-down list, select the Web service associated with the rule.

    In the Web service drop-down list, you can see the Display Name of the Web service. For more information, see Configuring Open Interfaces for email on page 285.
25. Click **Save**.

Variable definitions

Name	Description
Current Search Criteria	Select the criterion to configure for the rule. Choose Keyword Match to select a keyword group that contains phrases or words to search. Choose Sender Group to select an email address from which the email message is received. Choose a maximum of five criteria for each rule. **Note:** If you select multiple keyword groups that include an 'AND' statement, CCMM detects matches only if all keywords are found in either the subject or body of the email message. CCMM detects no match if some keywords are included in the body and some keywords are included in the subject.
Available Auto Responses	Select the automatic response that you can choose for the rule group. You can choose only one automatic response. Automatic responses under Available Auto Responses show what you can choose. The Automatic responses in the right column show the configuration for this rule.
Available Auto Suggests	Select the automatic suggestions that you can choose for the rule group. You can choose up to five automatic suggestions for future automatic suggestion promotion.

Table continues…

Name	Description
	Automatic suggestions under Available Auto Suggestions show what you can select. The automatic suggestions in the right column show the configuration for this rule.
Name	The name of the rule. The name must be unique and less than 64 characters.
Skillset	Select the name of the skillset to route contacts.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 10.
Will use office hours	Select the check box to use the office hours calendar to determine whether the contact center is open or closed.
Will close contact	Select the check box to close the contact when the rule is applied to the contact.
Call Open Interface web service	Select the check box to call a Web service.
Web Service	Select the Web service associated with the rule.

Enabling a rule

About this task

Rules can be enabled within a rule group.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Rule Groups**.
4. Select a disabled rule.
5. Under **Rules**, click the check mark (√) button.
6. Click **Save**.

Disabling a rule

About this task

Rules can be disabled within a rule group. You can disable the rule functionality without deleting the rule.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Rule Groups**.
4. Select an enabled rule.
5. Under **Rules**, click the cross (**X**) button.
6. Click **Save**.

Deleting a rule

Before you begin

- Create a rule.

About this task

Permanently delete a rule. After you delete the rule, you cannot use the rule for routing email messages.

You cannot delete the Default Rule.

If you permanently delete a rule, existing contacts for the rule can no longer be archived by rule and any Contacts by Rule reports no longer work. Avaya recommends that you archive all contacts associated with a rule before you delete the rule.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Rule Groups**.
4. Under **Rules**, select the name of the rule to delete.
5. Click the minus sign (**—**) button.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

7. Click **Save**.

Creating or changing rule groups

About this task

Create rule groups to apply to the recipient mailboxes and aliases in your contact center.

A rule is a mechanism to route contacts based on who sent the email (sender groups), to apply treatments based on the time a contact was received (office hours), or to route the contact based on words or phrases (keywords). A rule can also send an automatic response and require no interaction by an agent.

A rule group is an ordered collection of rules that are reviewed and compared to the incoming email in a particular order. Contacts that best match or first match the rule are assigned to the skillset based on the rule that routes the contact. The rule group contains the default rule which routes the contact if no other rule in the rule group matches the email message.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Rule Groups**.
4. Click **New**.
5. In the **Name** box, type the name of the new rule group.

   OR

   In the **Rule Groups** list, select the rule group to change.
6. Select the **Matching Type** for the rule group.
7. To add a new rule to the group, click the plus sign (**+**) button.
8. To remove a rule from the group, click the minus sign (**—**) button.
9. Configure the new rule using the input criteria, responses, and general settings.
10. To change the order of the rules in the group, select the rule, and then click the up arrow (**^**) button and down arrow (**v**) button to change the order of the rules.
11. Click **Save**.

Variable definitions

Name	Description
Matching Type	Choose the matching type. For Best match, the system checks all rules in the rule group and routes the email message according to the rule with the highest percentage match. For First match, the system checks one rule at a time, in the order of the rule group and routes the email message according to the rule that matches first.
Name	Name of the rule group. The name of the rule group must be unique and less than 64 characters.

Configuring supervisor approval for email messages on a per skillset basis

Before you begin

If you want to use keyword groups to reject email messages automatically, configure keyword groups. See Creating or changing a keyword group on page 256.

About this task

Supervisors can approve email messages before the email messages reach the customers.

Note:

The approval process applies to email contacts only and does not apply to other contact types such as Fax, Scanned Documents, and SMS.

You can configure Contact Center to send email messages to supervisors for approval on a per skillset basis or per agent basis.

You can configure up to five levels of supervisor approval before Contact Center sends the email messages to the customer. Contact Center offers the email message to a hierarchy of supervisors before the final approval is granted.

Note:

Under the following conditions, a contact can get held up in the approval process:

- an administrator deletes a skillset that is part of the supervisor approval chain and the contact is already in queue waiting for that skillset to come into service
- an administrator deletes the original agent and a supervisor rejects the email message
- an administrator deletes the supervisor who needs to approve the email message

In such situations, an agent must pull the contact using Agent Desktop.

For more information, see Supervisor approval of email messages on page 210 and Configuring supervisor approval for email messages on a per agent basis on page 365.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Supervisor Approvals**.
4. Select a skillset under Supervisor Approvals.
5. Click **Edit**.
6. From the drop-down list, under Approval Hierarchy, select the skillset for which you need supervisors to approve email messages.

   You can configure an approval hierarchy of up to five unique approval skillsets. You cannot configure a skillset to be approved by itself.

   Note:

   Agents can belong to the skillset that approves email messages. Therefore, you must configure the approval process in a way that restricts agents from approving email messages.
7. From the drop-down list, under Rejection Flow, select the rejection hierarchy for each approval level. You can select one of the following:
   - **Reject to original skillset**
   - Reject to current approval level –1. This hierarchy is the default setting. For example, **Reject to approval level 1**.

   You must configure a rejection hierarchy for each approval level. The rejection hierarchy controls the flow of email messages through the levels of approval skillsets for a rejected email message. For example, you can decide to automatically send all rejected email messages, at any level, back to the originator.
8. In the **Approval Ratio** field, type the percentage of email messages that require supervisor approval for that skillset.

   The approval ratio must be whole numbers ranging from 0 to 100.
9. **(Optional)** From the **Auto-Rejection Keyword Group** drop-down list, select a keyword group based on which the system automatically rejects the email messages for that skillset.
10. **(Optional)** To create a new keyword group, click the plus (**+**) button next to the **Auto-Rejection Keyword Group** drop-down list. The system uses the new keyword group to automatically reject email messages for that skillset.
11. Click **Save**.

Next steps

Optionally, you can configure Contact Center to auto-reject contacts on all the skillsets configured for supervisor approvals, based on a single keyword group. For more information, see Configuring auto-rejection of email messages from all skillsets that use approval hierarchy on page 273.

Configuring auto-rejection of email messages from all skillsets that use approval hierarchy

Before you begin

- Configure your keyword groups. See Creating or changing a keyword group on page 256.
- Configure supervisor approval on one or more skillsets.

About this task

If you have set up supervisor approval of email messages, you can configure Contact Center to use a keyword group to automatically reject email messages from all the skillsets that use approval hierarchy.

For example, you can configure a keyword group named Abusive, and then add a list of abusive words to the group. For all skillsets that use approval hierarchy, Contact Center automatically rejects email messages that contain words listed in the Abusive keyword group. This configuration does not affect skillsets that do not have an approval hierarchy.

Note:

Auto-rejection of email messages applies to the first approval level prior to the first review by a supervisor. After a supervisor reviews an email message, auto-rejection of email messages is not applicable.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Supervisor Approvals**.
4. Under Global Settings, in the **Auto-Rejection Keyword Group For All Skillsets** drop-down list, select a keyword group based on which Contact Center rejects email messages automatically.
5. Review the list of skillsets, and ensure that the skillsets to which you want the auto-rejection keyword group to apply have an approval hierarchy.
6. Click **Save**.

Configuring the email settings

About this task

Configure the following email settings for email messages entering and leaving your designated contact center mailboxes:

- how frequently you scan the email server for new messages
- the location in which attachments are stored
- automatic numbering of email messages
- which text is searched when you use keywords for rules

Default values are provided for required fields. You can change or accept the default values for the optional settings.

Procedure

1. Open the Multimedia Administration utility.
2. In the left pane, click **E-mail**.
3. Click **General Settings**.
4. To change the attachment file location from the file system to the database, select **Store in the database**.
5. To change the attachment file locations on the file system, under **Attachment Files**, type the new paths for the inbound and outbound URL and shared folders into the fields provided.
6. To configure a mailbox scan interval, under **Mailbox Scan Interval**, in the **Interval** box, type the time in minutes.
7. To include the customer ID or contact ID in a number for the outgoing email message numbering, under **Message Properties**, select the **Customer ID** check box, the **Contact ID** check box, or both.
8. To include the email message body in the keyword search, select the **Include email body in keyword search** check box.
9. Click **Save**.

Variable definitions

Name	Description
Interval	The interval between mailbox scans to check for new incoming email messages. You can specify minutes and seconds between each scan.

Table continues…

Name	Description
Store in the database	Select the check box to save new attachments in the MULTIMEDIA database instead of on the file system.
Inbound Url	The uniform resource locator (URL) that shows the location of the inbound email attachments. When Web Services security is on, use https as the URL prefix. If you have turned off Web Services security, use http as the URL prefix.
Inbound Share	The path of the shared folder on the Contact Center Multimedia server in which the inbound email attachments are stored.
Outbound Url	The uniform resource locator (URL) that shows the location of the outbound email attachments. When Web Services security is on, use https as the URL prefix. If you have turned off Web Services security, use http as the URL prefix.
Outbound Share	The path of the shared folder on the Contact Center Multimedia server in which the outbound email attachments are stored.
Autonumber outgoing email	Select the check box to number the email message automatically with either the customer ID, the contact ID, or both. The number appears in the subject of the message for identification.
Include email body in keyword search	Select the check box to enable a keyword search in both the subject and the body of the email message.
Search for first characters	Specify the number of characters in the content of the body of the email message that you search for keywords if you enabled the keyword search in the body of the email message.

Changing the character encoding for outgoing and incoming email

Before you begin

- Avaya recommends that only contact centers in Europe use Latin-9 encoding.

About this task

Change the character encoding of outgoing email to reply to an email message by using the same character set as the inbound email. For example, if an email arrives at the contact center with

Latin-1 encoding, the reply from the Agent Desktop or the automatic response is sent in Latin-1. The customer email client can understand the format of the message sent from the contact center.

Use Latin-9 to provide support for the Euro currency symbol, as this character is not included in the Latin-1 character set. Outgoing email messages encoded in Latin-1 that include the Euro symbol, deliver the symbol as a question mark. However, not all recipient clients understand Latin-9 and can receive what is perceived as a blank email message. Therefore, Avaya recommends that contact centers in Europe use the option for Latin-9 encoding while contact centers outside Europe avoid it.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **General Settings**.
4. In the **Encoding for agent initiated emails** list, select the type of character encoding to use.
5. To use Latin-9 encoding for replies, under **Customer Replies**, select the **Reply to Latin 1 as Latin 9** check box.
6. Click **Save**.
7. On the Contact Center Multimedia server, on the **Start** screen click **Administrative Tools** > **Services**.
8. Right-click **CCMM Email Manager.**
9. Click **Restart**.
10. Close the Services window.

Selecting the outgoing email address

Before you begin

- Configure the email mailbox from which to send outbound email messages. See Creating or changing a recipient mailbox on page 247.

About this task

You can send email messages from the email address to which the original message was sent or from a general email address in the contact center.

You can choose the response email address based on a skillset.

Note:

This procedure does not apply to automatic responses. Contact Center sends all automatic responses from the email address that the incoming email message was sent to.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Outgoing E-mail**.
4. On the **Skillset to Mailbox Mappings** tab, select a skillset.
5. Click **Edit**.
6. In the **Address** box, select the address from which you want email messages sent from this skillset.
7. To send customer responses from an address specified for the skillset, click **Send both Agent-Initiated Contacts and Customer Responses from this e-mail address**.
8. To send customer responses from the address that the customer used, click **Respond to Customer Contacts with the Recipient address of the original e-mail, and send Agent-Initiated Contacts from this address**.
9. Click **Save**.

Barring email addresses

About this task

Configure Contact Center Multimedia to block certain email addresses. When you bar an email address, automatic replies, and agent email messages are not sent to the barred address.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Outgoing E-mail**.
4. Click the **Barred Outgoing Addresses** tab.
5. Click **New**.

   OR

   Select an existing barred email address, and then click **Edit**.
6. In the **Address** box, type the email address to block.
7. Click **Save**.

   The address appears in the list of Barred Addresses.

Deleting a barred email address

Before you begin

- Ensure that removing a barred address does not violate local governing for do-not-call lists.

About this task

Remove a blocked email address from the barred email address list.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Outgoing E-mail**.
4. Click the **Barred Outgoing Addresses** tab.
5. Select a barred email address from the list provided.
6. Click **Delete**.

   The system displays a Warning dialog box.
7. Click **Yes** to confirm the deletion.

Configuring Microsoft Exchange for sending outgoing email

Before you begin

- Ensure that you use Microsoft Exchange on your email server.

About this task

Configure Microsoft Exchange to send outgoing email messages from Agent Desktop.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **General Administration**.
3. Click **Server Settings**.
4. Select **Outbound Mail Server (SMTP)**.
5. Click **Edit**.
6. Under **Advanced SMTP Authentication**, select **Base 64 Encoded Authentication**.
7. Click **Save**.

8. Close the Contact Center Manager Administration window.
9. Log on to the Microsoft Exchange server.
10. Open the Exchange Management Console.
11. Click **Server Configuration** > **Hub Transport** > **Receive Connectors Tab**.
12. Right-click **Default <Servername>** and select **Properties**.
13. Click the **Authentication** tab.
14. Disable all authentication options except for the following:
    - Basic Authentication
    - Exchange Server Authentication
    - Integrated Windows Authentication
15. Click **OK**.
16. If you are using Microsoft Exchange 2007, close the Exchange Management Console and skip the remainder of this procedure.
17. Click **Server Configuration** > **Client Access**.
18. Click the **POP3 and IMAP4** tab.
19. Right-click **POP3** and select **Properties**.
20. Click the **Authentication** tab.
21. Under **Logon Method**, select **Plain text logon (Basic authentication). No TLS connection is required for the client to authenticate to the server**.
22. Click **OK**.
23. Close the Exchange Management Console.
24. On your Microsoft Exchange server, click **Start** > **Administrative Tools** > **Services**.
25. In the **Services** window, right-click the **Microsoft Exchange POP3** icon and select **Restart**.
26. Close the **Services** window.

Adding a certificate for use with TLS email connections

Before you begin

- Avaya recommends that you use a false connection on the fallback. If you assign fallback to false, a secure connection cannot be established and the operation fails. If you assign the fallback to true, during a failure the connection is insecure.

About this task

Enable Transport Layer Security (TLS) on the Email Manager. Contact Center Multimedia supports TLS to protect data traveling between the email server and the Contact Center Multimedia server.

Although SMTP is secure, when email traverses the Internet, it becomes insecure. Implementations of secure SMTP vary as does the port number. For more information, see the documentation for your email server.

The following error can occur:

```
EmailManager.log file javax.net.ssl.SSLHandshakeException: Could not
find trusted certificate.
```

This message indicates that the target mail server TLS certificate was signed with a certificate from a signing authority that is not trusted, or that you are using a test certificate and must enable SMTP Authentication on your email server.

Note:

Contact Center supports monitored mailboxes distributed across several email servers.

Use the Java keytool to enable trust for a signing authorities certificate. By default, Java applicationTLS implementations automatically trust many of the major certificate authorities such as Verisign or Thawte.

Procedure

1. Copy the certificate file into the following directory:

   `C:\Program Files (x86)\Zulu\zulu-8-jre\lib\security`

2. On the **Desktop** screen, click **Start** > **Command Prompt**.
3. Use the following CD command to change to the Java security certificates directory:

   ```
   CD "C:\Program Files (x86)\Zulu\zulu-8-jre\lib\security"
   ```

4. Enter the following command:

   ```
   keytool -importcert -alias <mycacert> -file <mycacert>.cer -keystore cacerts
   ```

   Where <*mycacert*> is the name of your certificate file.

5. After the Java keytool prompts you for a keystore password, enter the default installation password for the JRE trust keystore, `changeit`.

   After the Java keytool prints the certificate details, the Java keytool prompts you to trust this certificate.

6. Type `yes`, and then press `Enter` to update the keystore.

   The file appears, similar to the following example:

   ```
   Owner: OU=For VeriSign authorized testing only. No
   assurances (C)VS1997, OU=www.verisign.com/repository/
   TestCPS Incorp. By Ref. Liab. LTD., O="VeriSign, Inc"
   Issuer: OU=For VeriSign authorized testing only. No
   assurances (C)VS1997, OU=www.verisign.com/repository/
   TestCPS Incorp. By Ref. Liab. LTD., O="VeriSign, Inc"
   Serial number: 52a9f424da674c9daf4f537852abef6e
   ```

```
Valid from: Sun Jun 07 01:00:00 BST 1998 until: Wed Jun
07 00:59:59 BST 2006
Certificate fingerprints:
MD5:
40:06:53:11:FD:B3:3E:88:0A:6F:7D:D1:4E:22:91:87
SHA1:
93:71:C9:EE:57:09:92:5D:0A:8E:FA:02:0B:E2:F5:E6:98:6C:6
0:DE
Trust this certificate? [no]: y
Certificate was added to keystore
```

7. Enter the keystore password `changeit`.
8. Restart the **Email Manager** service.
9. To change the default password for security reasons, type the following command and enter a new password:

```
keytool -storepasswd -new changeit -keystore
C:\Program Files (x86)\Zulu\zulu-8-jre\lib\security\cacerts
```

Enabling SMTP Authentication on your email server

About this task

Enable SMTP authentication for Microsoft Exchange Server. SMTP Authentication is a mechanism to restrict non-authenticated clients from sending email messages outside your organization. Agents who want to send external email messages must provide their logon credentials to the email server before their email is relayed. Failure to authenticate leads to an immediate message from the email server indicating that sending the email is prohibited or a later non-delivery report email. Organizations generally implement SMTP authentication to prevent SPAM messages from being relayed through the networks. For more information, see the Microsoft Knowledge Base article Q197869.

SMTP authentication varies among email servers.

Procedure

1. Log on to the **Microsoft Exchange Server** with domain administrative privileges.
2. Start the **Microsoft Exchange Administrator** program.
3. On the **Configuration** branch, double-click **Internet Mail Service**.
4. On the **Routing** tab, click **Routing Restrictions**.
5. Ensure you select the **Only Hosts and Clients who successfully authenticate** check box.
6. Restart the **Microsoft Exchange Internet Mail Service**.

Determining if SMTP Authentication is enabled

About this task

Use Telnet to verify whether the server response to the SMTP commands is enabled on an email server.

After a successful logon, you can send an email message using the MAIL, RCPT, and DATA commands.

Procedure

1. Start Telnet and connect to the IP Address or host name of the mail server. Connect using the well-known port for SMTP (Port 25). Ensure that your Telnet application is enabling a local echo.

   The following message appears:

   ```
   220 SERVERNAME.DOMAIN.COM ESMTP Server (Microsoft
   Exchange
   Internet Mail Service 5.5.2650.21) ready
   ```

2. Type `HELO`.
3. Try to send an email message to an external address using the MAIL command:

   ```
   MAIL FROM: anymailbox
   250 OK - mail from <anymailbox>
   ```

4. Specify recipients using the RCPT command.

   If SMTP Authentication is enabled, you see the following message:

   ```
   RCPT TO: anyone@externaladdress.com
   550 Relaying is prohibited
   ```

   Otherwise, you receive the following message:

   ```
   RCPT TO: anyone@externaladdress.com
   250 OK - Recipient <anyone@externaladdress.com>
   ```

5. If you find that SMTP Authentication is not enabled, you can continue to send an email message using the DATA command:

   ```
   DATA
   354 Send data. End with CRLF.CRLF
   ```

6. Conclude the email message by typing `<ENTER> . <ENTER>`

   The email message is sent.

   `250 OK`

7. If the SMTP Authentication is enabled, you must reconnect to your email server.

8. Enter the EHLO command after you reconnect:

```
EHLO
250-SERVERNAME.DOMAIN.COM Hello [LocalMachineName]
250-XEXCH50
250-HELP
250-ETRN
250-DSN
250-SIZE 0
250-AUTH LOGIN
250 AUTH=LOGIN
```

9. Type the AUTH LOGIN command:

```
AUTH LOGIN
334 VXNlcm5hbWU6
```

10. Type your user name encoded using Base64.

    A base64 encoded prompt for password appears:

```
AUTH LOGIN
334 VXNlcm5hbWU6
dGVzdA==
334 UGFzc3dvcmQ6
dGVzdA==
235 LOGIN authentication successful
```

Important:

dGVzdA== represents the word *test* when base64-encoded. The responses shown here are examples. Use the base64 representation of your user name and password that is specific to your email mailbox account.

11. Confirm the user name and password.

Adding an email address of an administrator in CCMM Dashboard

Before you begin

- Ensure that the Extended Email Capacity feature is disabled in Contact Center.

About this task

Add an email address of an administrator so that the administrator receives notifications when the number of email messages in the queue is approaching the threshold. If the number of email messages that have the New status is more than 10 000 in a standalone CCMM configuration and 4 000 in a coresident configuration, Email Manager sends an email to the administrator to enable the Extended Email Capacity feature.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Multimedia Dashboard**.

2. In the **Administrator e-mail address (for notifications)** field, type the email address of the administrator to whom you want Email Manager to send notification messages.
3. Click **Save**.

Enabling Extended Email Capacity

Before you begin

- Ensure that you configure your multicast IP address.
- Log on to CCMA from a Web browser opened on the CCMM server.

About this task

The Extended Email Capacity feature increases the email backlog capacity to 100 000. Enable the Extended Email Capacity feature if you want to increase the email backlog capacity to more than 20 000. For more information, see Extended Email Capacity on page 209.

While enabling the Extended Email Capacity feature, you can select the order in which the system queues the contacts to skillsets, either by priority first or by age first.

Note:

After you enable the Extended Email Capacity feature, you can disable this feature only if the number of contacts in the Open or Waiting status is less than the Maximum Open Contacts Threshold. The Maximum Open Contacts Threshold is 19 000 in a standalone CCMM configuration and 4 000 in a coresident configuration.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **General Settings**.
4. Click **Advanced**.

   The system displays the Advanced Email Configuration dialog box.
5. Select the **Enable Extended E-mail Capacity** check box.
6. In the **E-mail Queue Preference** field, select the order in which the system queues the contacts. You can queue the contacts in one of the following ways:
   - **By priority first, then age**
   - **By age first, then priority**
7. Click **Save**.

Disabling Extended Email Capacity

Before you begin

Log on to CCMA from a Web browser opened on the CCMM server.

About this task

You can disable the Extended Email Capacity feature only if the number of contacts in the Open or Waiting status is less than the Maximum Open Contacts Threshold, which is 19 000 in a standalone CCMM configuration and 4 000 in a coresident configuration. For more information, see Extended Email Capacity on page 209.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **General Settings**.
4. Click **Advanced**.

   The system displays the Advanced Email Configuration dialog box.
5. Clear the **Enable Extended E-mail Capacity** check box.
6. Click **Save**.

Configuring Open Interfaces for email

Before you begin

Ensure that the rule that is associated with the Web service is set up. For more information, see Creating or changing rules on page 265.

About this task

Use the Multimedia Administration utility to configure a custom Web service, which conforms to the Web Service Description Language (WSDL) standards. You must enter the URL of the WSDL and method names, provide other necessary properties, and specify the input and output parameters. For more information, see Open Interfaces for email on page 213.

The Email Open Interfaces package in the Email Manager dynamically creates a Web service client based on WSDL that you specify.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Open Interfaces**.

4. Click **New**.
5. In the **WSDL URL** field, type the URL for the WSDL.
6. Click the **Discover** button.

   The **Discover** button sends a query to the WSDL URL and lists the methods retrieved from the URL

   The system displays the Open Interfaces method discovery dialog box.
7. In the Open Interfaces method discovery dialog box, select the methods that you want to add to the Web service.
8. Click **Add** to add the selected methods, or click **Add all** to add all the methods.

   The system displays the methods selected under the Methods section.
9. To add a new method, click **New** under the Methods section.

   Or

   To edit an existing method, click **Edit** under the Methods section.
10. In the **Method** field, type the method name.
11. In the **Display Name** field, type the name that you want to display for the method.

    Note:

    The display name must be unique across all Web services.
12. In the Input Parameters section, click the right arrow (**>**) to move the selected parameter to the list of parameters to be passed to the Web method.

    The input parameter list is a static list of the fields from the email. You can select the parameters that are passed to the Web service.

    To remove a parameter, select the parameter, and then click the left arrow (**<**) to remove it from the input parameter list.
13. In the Output Parameters section, click the right arrow (**>**) to move the selected parameter to the list of parameters to be returned from the Web service.

    The output parameters replace or complement the original rule output. For example, the Web service can determine a different skillset or priority for the email, manipulate the body of the email, or return a screen pop or knowledge base links.

    To remove a parameter, select the parameter, and then click the left arrow (**<**) to remove it from the output parameter list.
14. Click **Save**.
15. Click **Save**.

Variable definitions

Name	Description
WSDL URL	The URL for the WSDL.
Method	The name of the method.
Display Name	The name that you want to display for the method. The display name must be unique across all Web services.
Input Parameters	The input parameter list is a static list of the fields from the email. You can select the parameters that are passed to the Web service. Input parameters are: • Mailstore • To Address • To Address List • CC Address List • From Address • Subject • Plain Text Body • HTML Body • E-mail headers
Output Parameters	The list of parameters to be returned from the Web service. You can select the parameters that are returned from the Web service. Output parameters are: • To Address List • CC Address List • Subject • Plain Text Body • HTML Body • Skillset • Priority • Customer ID • CustomField Name • CustomField Value

Table continues…

Name	Description
	• From Address • Agent ID • Auto-close

Disabling email retrieval for all mailboxes

About this task

You can disable email retrieval for all mailboxes in Contact Center. One important use of disabling email retrieval is when you want to turn Extended Email Capacity off. When you want to turn Extended Email Capacity off, agents have to quickly close the new incoming mail contacts to get the total number of contacts in the Open or Waiting status less than the number set in the Maximum Open Contacts Threshold. The Maximum Open Contacts Threshold is 19 000 in a standalone CCMM configuration and 4 000 in a coresident configuration.

If you disable email retrieval for all mailboxes, the agents can work through the email messages backlog, and you can turn Extended Email Capacity off.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Recipient Addresses**.
4. Click **Disable All**.

   The system displays a Warning dialog box.
5. Click **Yes**.

   The system disables email retrieval for all mailboxes.

Reenabling email retrieval for all mailboxes

Before you begin

- Ensure that email retrieval for all mailboxes is disabled. For more information, see Disabling email retrieval for all mailboxes on page 288.

About this task

If you have disabled email retrieval for all mailboxes earlier, you can reenable email retrieval for all mailboxes in Contact Center.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **E-mail**.
3. Click **Recipient Addresses**.
4. Click **Enable All**.

   The system displays a Warning dialog box.
5. Click **Yes**.

   The system reenables email retrieval for all mailboxes.

Chapter 26: Voice mail configuration

This chapter contains the configuration steps for the voice mail recipient mailbox and routing voice mail contacts.

In the contact center, the recipient mailboxes are polled for incoming voice mail messages. A voice mail server forwards voice mail messages to an email address. The Contact Center Multimedia Email Manager retrieves the voice mail (.wav) attachment and queues it to the appropriate skillset with an assigned priority. The caller ID is extracted to facilitate callbacks to the customer.

Reports appear in the Contact Center Multimedia Administration utility to show the current status of the voice mail traffic. The following reports appear when you select Voice Mail and View Reports in the left column of the Contact Center Multimedia application. You can choose the report date and the skillsets represented in all displayed real-time reports.

- The Voice Mail (New Vs. Closed) report shows the number of contacts in a new and closed state against the time for the selected date and skillsets.
- The Voice Mail Progress report shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for that date.
- The Voice Mail Closed Contacts Queue Time report shows the average time a voice mail contact spends in queue while the contact center is open.

Note:

Voice mail configuration procedures do not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Prerequisites for voice mail configuration

Procedure

Ensure that you are licensed for email contacts.

Configuring a route point for a voice mail skillset

About this task

Configure a route point for a voice mail skillset to route voice mail contacts to a particular agent. Skillsets are used to assign contacts to agents.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. In the **Skillset Settings** dialog box, select the skillset to assign a route point.

   The skillset must have the prefix VM.
5. Under the **Edit Skillset** dialog box, in the **Route Point** list, select the route point to assign to the voice mail skillset.
6. Click **Save**.

Variable definitions

Name	Description
Route point	A location in the open queue that enables incoming contacts to queue and run through a script on the Contact Center Manager Server.

Adding a voice mail server

About this task

Add the voice mail server for your Contact Center Multimedia server as per your requirement.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Voice Mail**.
3. Click **Mailbox Configuration**.
4. Click **Voice Mail Server** (image).
5. In the Voice Mail Server Configuration window, click **Add**.

6. In the **Voice Mail Server Hostname** box, type the name of the new server.
7. In the **Type** box, select the type of server.
8. Click **Save**.

Updating a voice mail server

About this task

Update the voice mail server for your Contact Center Multimedia server as per your requirement.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Voice Mail**.
3. Click **Mailbox Configuration**.
4. Click **Voice Mail Server** (image).
5. In the Voice Mail Server Configuration window, click **Edit**.
6. Change the properties of your Voice Mail server, as required.
7. Click **Save**.

Deleting a voice mail server

About this task

Delete the voice mail server for your Contact Center Multimedia server if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Voice Mail**.
3. Click **Mailbox Configuration**.
4. Click **Voice Mail Server** (image).
5. In the Voice Mail Server Configuration window, select the server that you want to and click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the server deletion.

7. Click **Close**.

Adding a voice mail mailbox

Before you begin

- Configure a skillset for a voice mail contact.

Important:

You must configure the voice mail server, Avaya CallPilot®, the email server, and a recipient mailbox in Contact Center to receive voice mail messages in the contact center.

About this task

Add a voice mail mailbox to the multimedia configuration for receiving voice mail messages as .wav attachments.

Also, choose the skillset for the mailbox so that the voice mail message is routed to the agent who has the best skills to handle the specific contact.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Voice Mail**.
3. Click **Mailbox Configuration**.
4. Click **Add**.
5. On the **Mailbox** tab, in the **Inbound Server** field, select the host name of your POP3 or IMAP server along with the respective security protocol.
6. In the **Outbound Server** field, select the host name of your SMTP server.
7. In the **Mailbox** field, type the mailbox name.
8. In the **Domain** field, type the mailbox domain.
9. In the **Password** and **Confirm** boxes, type and retype the password to access the mailbox.
10. In the **Skillset** field, choose a configured skillset for routing the voice mail contacts.
11. In the **Contact Priority** field, choose a priority for voice mail contacts received in this mailbox.
12. Click the **Sender Address** tab.
13. Select **Use full sender address** or **Parse sender address for CLID**.
14. If you select **Parse sender address for CLID**, then in the **Leading Characters to Remove** field, type the characters that you must not dial when making the outgoing callback.

15. Click **Save**.

Variable definitions

Name	Description
Inbound Server	The host name of the email server that handles email messages that enter the contact center.
Outbound Server	The host name of the email server that delivers email messages that leave the contact center.
Mailbox	Name of the mailbox on the email server that is polled for new incoming email messages.
Domain	The domain name for the email server.
Password	The password used to access the mailbox on the email server. Type the password in the Confirm Password box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager Server database. You must select a route point for a skillset used to route voice mail contacts.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 6. For example, a call with priority 1 is handled before a call with priority 6.
Sender address	Select Use full sender address or Parse the address for the Calling Line identification (CLID) to save for future contacts. The address in the format you select is stored with the contact for future communication with the customer.
Leading characters to remove	If you select a Calling Line Identification (CLID) to add the customer's phone number into the contact information, type any leading characters or trunk numbers to remove from the current number.

Updating a voice mail mailbox

Before you begin

- Add a voice mail mailbox.

About this task

Update the properties of the voice mail mailbox, as per your requirements.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Voice Mail**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be edited.
5. Click **Edit**.
6. Update the mailbox settings as required.
7. Click **Save**.

Deleting a voice mail mailbox

Before you begin

- Add a voice mail mailbox.

About this task

Delete a voice mail mailbox, if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Voice Mail**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Updating the voice mail system default rule

Before you begin

- Ensure that you know the default settings for the system delivery failure rule:
  - use the voice mail default skillset, VM_Default_Skillset
  - use no automatic response
  - assign priority 3
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, VM_Default_Skillset is used.
- Configure the route points for the skillset you assign to the system default rule. For more information, see Configuring a route point for a voice mail skillset on page 291.

About this task

Update the voice mail system default rule to ensure that email messages received with voice mail attachments are routed to an agent if no other rule associated to the recipient mailbox routes the email message.

The system default rule is used in every rule group configured in Contact Center Multimedia.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Voice Mail**.
3. Click **Default Rules**.
4. Under **System Default Rule**, from the **Skillset** list, select a skillset name to assign to the contact.
5. Under **System Default Rule**, from the **Priority** list, select the priority to assign to the contact.
6. Click **Save**.

Variable definitions

Name	Description
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact

Table continues…

Name	Description
	Center Manager Server database. You must select a route point for a skillset used to route contacts.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 10. For example, a call with priority 1 is handled before a call with priority 10.

Updating the voice mail system delivery failure rule

Before you begin

- Ensure that you are licensed to handle email messages.
- Ensure that you know the default settings for the system delivery failure rule:
  - use the voice mail default skillset, VM_Default _Skillset
  - use keyword group delivery failure keywords
  - assign priority 10 (lowest)
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, VM_Default_Skillset is used.
- Configure the route point for the skillset you plan to assign to the system delivery failure rule. See Configuring a route point for a voice mail skillset on page 291.

About this task

Update the voice mail system delivery failure rule to ensure that any email message that contains particular phrases such as undeliverable, returned mail, unknown recipient, delivery failure, or delivery report is deleted and not assigned to an agent.

When you create a recipient mailbox, the system delivery failure rule is copied as the first regular rule into list of rules for the recipient mailbox.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Voice Mail**.
3. Under **System Delivery Failure Rule**, from the **Skillset** list, select a skillset name to assign to the contact.
4. To change the keyword group, select the keyword group which contains the delivery failure keywords from the **Keyword Group** list under the **System Delivery Failure Rule**.

5. To change the priority, under **Priority**, select the priority to assign to the contact from the **Priority** list under the **System Delivery Failure Rule**.
6. To close contacts matching the delivery failure keywords, select the **Will close contact** check box.
7. Click **Save**.

Variable definitions

Name	Description
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager Server database. You must select a route point for a skillset used to route outbound contacts.
Keyword group	A list of words that you can search in an email message. Keyword groups associate keywords and expressions considered important by the contact center to be handled in a particular way.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 10. For example, a call with priority 1 is handled before a call with priority 10.
Will close contact	Select the check box to close the email contact after the system delivery failure rule determines that the contact is not appropriate for the contact center. Clear the check box to leave the email contact open for review.

Chapter 27: Scanned document configuration

This chapter contains the configuration steps for the recipient mailbox that receives scanned documents.

In the contact center, the recipient mailboxes are polled for incoming scanned documents. A server forwards scanned documents to an email address. The Contact Center Multimedia Email Manager retrieves the scanned document as an attachment (.tiff) and queues it to the appropriate skillset with an assigned priority.

Reports appear in the Contact Center Multimedia Administration utility to show the current status of the contact type traffic. The following reports appear when you select Scanned Documents and View Reports in the left column of the Contact Center Multimedia application. You can choose the report date and the skillsets represented in all displayed real time reports.

- The Scanned Document (New Vs. Closed) report shows the number of contacts in a new and closed state against the time for the selected date and skillsets.
- The Scanned Document Progress report shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for that date.
- The Scanned Document Closed Contacts Queue Time report shows the average time a contact spends in queue while the contact center is open.

Note:

Scanned document configuration procedures do not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Prerequisites for scanned document configuration

Procedure

Ensure that you are licensed for email contacts.

Configuring a route point for a scanned document skillset

About this task

Configure a route point for a scanned document skillset to route the contact to a particular agent. Skillsets are used to assign the contacts to agents.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. In the **Skillset Settings** dialog box, select the skillset to assign a route point.

   The skillset must have the prefix SD.
5. Under the **Edit Skillset** dialog box, in the **Route Point** list, select the route point to assign to the scanned document skillset.
6. Click **Save**.

Variable definitions

Name	Description
Route point	A location in the open queue that enables incoming contacts to queue and run through a script on the Contact Center Manager Server.

Adding a document imaging server

About this task

Add the document imaging server for your Contact Center Multimedia server as per your requirement.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Scanned Documents**.
3. Click **Mailbox Configuration**.
4. Click **Document Imaging Server** (image).
5. In the Document Imaging Server Configuration window, click **Add**.

6. In the **Document Server Hostname** box, type the name of the new server.
7. In the **Type** box, select the type of server.
8. Click **Save**.

Updating a document imaging server

About this task

Update the document imaging server for your Contact Center Multimedia server as per your requirement.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Scanned Documents**.
3. Click **Mailbox Configuration**.
4. Click **Document Imaging Server** (image).
5. In the Document Server Configuration window, select the server you are updating and click **Edit**.
6. Change the properties of your document imaging server.
7. Click **Save**.

Deleting a document imaging server

About this task

Delete the document imaging server for your Contact Center Multimedia server if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Scanned Documents**.
3. Click **Mailbox Configuration**.
4. Click **Document Imaging Server**.
5. In the Document Server Configuration window, select the server that you want to and click **Delete**.

The system displays a Warning dialog box.

6. Click **Yes** to confirm the deletion.
7. Click **Close**.

Adding a scanned document mailbox

Before you begin

- Configure a skillset for a scanned document.

About this task

Add a scanned document mailbox to the multimedia configuration for receiving scanned documents as .tiff attachments.

Also, choose the skillset for the mailbox so that the scanned document is routed to the agent who has the optimal skillset to handle the specific contact.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Scanned Document**.
3. Click **Mailbox Configuration**.
4. Click **Add**.
5. On the **Mailbox** tab, in the **Inbound Server** field, select the host name of your POP3 or IMAP server along with the respective security protocol.
6. In the **Outbound Server** field, select the host name of your SMTP server.
7. In the **Mailbox** field, type the mailbox name.
8. In the **Domain** field, type the mailbox domain.
9. In the **Password** and **Confirm** fields, type and retype the password to access the mailbox.
10. In the **Skillset** field, choose a configured skillset for routing the contact.
11. In the **Contact Priority** field, choose a priority for contacts received in this mailbox.
12. Click **Save**.

Variable definitions

Name	Description
Inbound Server	The host name of the email server that handles email messages entering the contact center.
Outbound Server	The host name of the email server that delivers email messages that leave the contact center.
Mailbox	Name of the mailbox on the email server that is polled for new incoming email messages.
Domain	The domain name for the email server.
Password	The password used to access the mailbox on the email server. Type the password in the Confirm box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager Server database. You must select a route point for a skillset used to route contacts.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 6. For example, a call with priority 1 is handled before a call with priority 6.

Updating a scanned document mailbox

Before you begin

- Add a scanned document mailbox.

About this task

Update the properties of the scanned document mailbox, as per your requirements.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Scanned Document**.
3. Click **Mailbox Configuration**.

4. Select the mailbox to be edited.
5. Click **Edit**.
6. Update the mailbox settings as required.
7. Click **Save**.

Deleting a scanned document mailbox

Before you begin

- Add a scanned document mailbox.

Important:

A scanned document mailbox cannot be deleted if it is currently assigned to a skillset

About this task

Delete a scanned document mailbox, if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Scanned Document**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Configuring a scanned document reply mailbox

About this task

Configure the reply information to the scanned document received by your contact center.

Configure the outgoing mailbox properties with a signature related to the skillset for replying to scanned document.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.

2. In the left pane, select **Scanned Document**.
3. Click **Reply Configuration**.
4. Under **Skillsets**, select a scanned document skillset for the mailbox configuration.
5. Under **Mailbox**, select a configured mailbox.

   OR

   Click **New** to create a new mailbox.

   OR

   Click **Edit** to edit an existing mailbox.
6. In the **SMTP Server** box, select the SMTP server to use for outgoing email messages.
7. In the **Mailbox** box, specify the new mailbox or change the name of the existing mailbox.
8. In the **Domain** box, type the email server domain.
9. In the **Password** and **Confirm** boxes, type and retype the email server password.
10. To use a different user name for the SMTP authentication, select the **Use Alternative username for SMTP Authentication** check box.
11. In the **Username** box, type the alternative user name.
12. Click **Save**.

Variable definitions

Name	Description
SMTP Server	The name of the email server that handles email messages leaving the contact center.
Mailbox	Name of the mailbox on the email server polled for email messages.
Domain	The domain name for the email server.
Password	The password used to access the mailbox on the email server. Type the password in the Confirm box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.
Use Alternative username for SMTP Authentication	If SMTP authentication is required for your outbound email server, select the user name for the authentication.

Deleting a scanned document reply mailbox

About this task

Delete a scanned document reply mailbox, if it is no longer required.

Important:

A scanned document reply mailbox cannot be deleted if it is currently assigned to a skillset.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Scanned Document**.
3. Click **Reply Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Updating the scanned documents system default rule

Before you begin

- Ensure that you know the default settings for the system delivery failure rule:
  - use the scanned documents default skillset, SD_Default_Skillset
  - use no automatic response
  - assign priority 3
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, SD_Default_Skillset is used.
- Configure the route points for the skillset you assign to the system default rule. For more information, see Configuring a route point for a scanned document skillset on page 300.

About this task

Update the scanned documents system default rule to ensure that email messages received with scanned document attachments are routed to an agent if no other rule associated to the recipient mailbox routes the email message.

The system default rule is used in every rule group configured in Contact Center Multimedia.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Scanned Documents**.
3. Click **Default Rules**.
4. Under **System Default Rule**, from the **Skillset** list, select a skillset name to assign to the contact.
5. Under **System Default Rule**, from the **Priority** list, select the priority to assign to the contact.
6. Click **Save**.

Updating the scanned documents system delivery failure rule

Before you begin

- Ensure that you are licensed to handle email messages.
- Ensure that you know the default settings for the system delivery failure rule:
  - use the scanned documents default skillset, SD_Default _Skillset
  - use keyword group delivery failure keywords
  - assign priority 10 (lowest)
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, SD_Default_Skillset is used.
- Configure the route point for the skillset you plan to assign to the system delivery failure rule. See Configuring a route point for a scanned document skillset on page 300.

About this task

Update the scanned documents system delivery failure rule to ensure that any email message that contains particular phrases such as undeliverable, returned mail, unknown recipient, delivery failure, or delivery report is deleted and not assigned to an agent.

When you create a recipient mailbox, the system delivery failure rule is copied as the first regular rule into list of rules for the recipient mailbox.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.

2. In the left pane, click **Scanned Documents**.
3. Under **System Delivery Failure Rule**, from the **Skillset** list, select a skillset name to assign to the contact.
4. To change the keyword group, select the keyword group which contains the delivery failure keywords from the **Keyword Group** list under the **System Delivery Failure Rule**.
5. To change the priority, under **Priority**, select the priority to assign to the contact from the **Priority** list under the **System Delivery Failure Rule**.
6. To close contacts matching the delivery failure keywords, select the **Will close contact** check box.
7. Click **Save**.

Chapter 28: Fax configuration

This chapter contains the configuration steps for the fax recipient mailbox.

In the contact center, the recipient mailboxes are polled for incoming fax messages. A fax server forwards messages to an email address. The Contact Center Multimedia Email Manager retrieves the fax attachment (.tiff) and queues it to the appropriate skillset with an assigned priority. The caller ID is extracted to facilitate callbacks to the customer.

Reports appear in the Contact Center Multimedia Administration utility to show the current status of the fax traffic. The following reports appear when you select Fax and View Reports in the left column of the Contact Center Multimedia application. You can choose the report date and the skillsets represented in all displayed real-time reports.

- The Fax (New Vs. Closed) report shows the number of contacts in a new and closed state against the time for the selected date and skillsets.
- The Fax Progress report shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for that date.
- The Fax Closed Contacts Queue Time report shows the average time a contact spends in queue while the contact center is open.

Note:

Fax configuration procedures do not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Prerequisites for fax configuration

Procedure

Ensure that you are licensed for email contacts.

Configuring a route point for a fax skillset

About this task

Configure a route point for a fax skillset to route fax contacts to a particular agent. Skillsets are used to assign the contacts to agents.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. In the **Skillset Settings** dialog box, select the skillset to assign a route point.

   The skillset must have the prefix FX.
5. Under the **Edit Skillset** dialog box, in the **Route Point** list, select the route point to assign to the fax skillset.
6. Click **Save**.

Variable definitions

Name	Description
Route point	A location in the open queue that enables incoming contacts to queue and run through a script on the Contact Center Manager Server.

Adding a fax server

About this task

Add the fax server for your Contact Center Multimedia server as per your requirement.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Fax**.
3. Click **Mailbox Configuration**.
4. Click **Fax Server** (image).
5. In the Fax Server Configuration window, click **Add**.
6. In the **Fax Server Hostname** box, type the name of the new server.
7. In the **Type** box, select the type of server.
8. Click **Save**.

Updating a fax server

About this task

Update the fax server for your Contact Center Multimedia server as per your requirement.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Fax**.
3. Click **Mailbox Configuration**.
4. Click **Fax Server** (image).
5. In the Fax Server Configuration window, click **Edit**.
6. Change the properties of your fax server.
7. Click **Save**.

Deleting a fax server

About this task

Delete the fax server for your Contact Center Multimedia server if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Fax**.
3. Click **Mailbox Configuration**.
4. Click **Fax Server**.
5. In the Fax Server Configuration window, select the server that you want to and click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.
7. Click **Close**.

Adding a fax mailbox

Before you begin

- Configure a skillset for a fax contact.

About this task

Add a fax mailbox to the multimedia configuration for receiving fax messages as .tiff attachments.

Also, choose the skillset for the mailbox so that the fax message is routed to the agent who has the optimal skillset to handle the specific contact.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Fax**.
3. Click **Mailbox Configuration**.
4. Click **Add**.
5. On the **Mailbox** tab, in the **Inbound Server** field, select the host name of your POP3 or IMAP server along with the respective security protocol.
6. In the **Outbound Server** field, select the host name of your SMTP server.
7. In the **Mailbox** field, type the mailbox name.
8. In the **Domain** field, type the mailbox domain.
9. In the **Password** and **Confirm** fields, type and retype the password to access the mailbox.
10. In the **Skillset** field, choose a configured skillset for routing the contacts.
11. In the **Contact Priority** field, choose a priority for contacts received in this mailbox.
12. Click the **Sender Address** tab.
13. Select **Use full sender address** or **Parse sender address for CLID**.
14. If you select **Parse sender address for CLID**, in the **Leading Characters to Remove** field, type the characters that you must not dial when making the outgoing callback.
15. Click **Save**.

Variable definitions

Name	Description
Inbound Server	The host name of the email server that handles email messages entering the contact center.

Table continues…

Name	Description
Outbound Server	The host name of the email server that delivers email messages that leave the contact center.
Mailbox	Name of the mailbox on the email server that is polled for new incoming email messages.
Domain	The domain name for the email server.
Password	The password used to access the mailbox on the email server. Type the password in the Confirm box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager Server database. You must select a route point for a skillset used to route contacts.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 6. For example, a call with priority 1 is handled before a call with priority 6.
Sender address	Select Use full sender address or Parse the address for the Calling Line identification (CLID) to save for future contacts. The address in the format you select is stored with the contact for future communication with the customer.
Leading characters to remove	If you select a Calling Line Identification (CLID) to add the customer's phone number into the contact information, type any leading characters or trunk numbers to remove from the current number.

Updating a fax mailbox

Before you begin

- Add a fax mailbox.

About this task

Update the properties of the fax mailbox, as per your requirements.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.

2. In the left pane, select **Fax**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be edited.
5. Click **Edit**.
6. Update the mailbox settings as required
7. Click **Save**.

Deleting a fax mailbox

Before you begin

- Add a fax mailbox.

Important:

A fax mailbox cannot be deleted if it is currently assigned to a skillset.

About this task

Delete a fax mailbox, if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Fax**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Configuring a fax reply mailbox

About this task

Configure the reply information for the fax message received by your contact center.

Configure the outgoing mailbox properties with a signature related to the skillset for replying to fax messages.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Fax**.
3. Click **Reply Configuration**.
4. Under **Skillsets**, select a fax skillset for the mailbox configuration.
5. Under **Mailbox**, select a configured mailbox.

   OR

   Click **New** to create a new mailbox.

   OR

   Click **Edit** to edit an existing mailbox.
6. In the **SMTP Server** box, select the SMTP server to use for outgoing email messages.
7. In the **Mailbox** box, specify the new mailbox or change the name of the existing mailbox.
8. In the **Domain** box, type the email server domain.
9. In the **Password** and **Confirm** boxes, type the email server password.
10. To use a different user name for the SMTP authentication, select the **Use Alternative username for SMTP Authentication** check box.
11. In the **Username** box, type the alternative user name.
12. Click **Save**.

Variable definitions

Name	Description
SMTP Server	The name of the email server that handles email messages leaving the contact center.
Mailbox	Name of the mailbox on the email server polled for email messages.
Domain	The domain name for the email server.
Password	The password used to access the mailbox on the email server. Type the password in the Confirm box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.
Use Alternative username for SMTP Authentication	If SMTP authentication is required for your outbound email server, select the user name for the authentication.

Deleting a fax reply mailbox

About this task

Delete a fax reply mailbox, if it is no longer required.

Important:

A fax reply mailbox cannot be deleted if it is currently assigned to a skillset.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Fax**.
3. Click **Reply Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Updating the fax system default rule

Before you begin

- Ensure that you know the default settings for the system delivery failure rule:
  - use the fax default skillset, FX_Default_Skillset
  - use no automatic response
  - assign priority 3
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, FX_Default_Skillset is used.
- Configure the route points for the skillset you assign to the system default rule. For more information, see Configuring a route point for a fax skillset on page 309.

About this task

Update the fax system default rule to ensure that email messages received with fax attachments are routed to an agent if no other rule associated to the recipient mailbox routes the email message.

The system default rule is used in every rule group configured in Contact Center Multimedia.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Fax**.
3. Click **Default Rules**.
4. Under **System Default Rule**, from the **Skillset** list, select a skillset name to assign to the contact.
5. Under **System Default Rule**, from the **Priority** list, select the priority to assign to the contact.
6. Click **Save**.

Updating the fax system delivery failure rule

Before you begin

- Ensure that you are licensed to handle email messages.
- Ensure that you know the default settings for the system delivery failure rule:
  - use the fax default skillset, FX_Default _Skillset
  - use keyword group delivery failure keywords
  - assign priority 10 (lowest)
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, FX_Default_Skillset is used.
- Configure the route point for the skillset you plan to assign to the system delivery failure rule. See Configuring a route point for a fax skillset on page 309.

About this task

Update the fax system delivery failure rule to ensure that any email message that contains particular phrases such as undeliverable, returned mail, unknown recipient, delivery failure, or delivery report is deleted and not assigned to an agent.

When you create a recipient mailbox, the system delivery failure rule is copied as the first regular rule into list of rules for the recipient mailbox.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Fax**.

3. Under **System Delivery Failure Rule**, from the **Skillset** list, select a skillset name to assign to the contact.
4. To change the keyword group, select the keyword group which contains the delivery failure keywords from the **Keyword Group** list under the **System Delivery Failure Rule**.
5. To change the priority, under **Priority**, select the priority to assign to the contact from the **Priority** list under the **System Delivery Failure Rule**.
6. To close contacts matching the delivery failure keywords, select the **Will close contact** check box.
7. Click **Save**.

Chapter 29: Social Network Configuration

Contact Center creates Social Networking contacts from email messages sent by Social Media Manager (SMM). Contact Center loads the email messages from defined mailboxes, and uses rules to queue the SN contacts to skillsets. Contact Center treats all emails in a defined mailbox as SN contacts—you cannot configure a mailbox for Social Networking if it was previously configured for another Multimedia contact type. Email Manager downloads and processes all the emails using the rules you define with the mailbox.

You can have multiple rules per mailbox. Each rule results in a skillset and priority for the contact. The rules use only the header values set and provided by SMM:

- Language
- Sentiment
- Channel
- Relevance

The rules implicitly use the logical AND condition when matching contacts: that is, the contact must match every condition set to satisfy the rule.

Contact Center processes the rules on a mailbox in the order in which you configure them. For a new email from SMM, Contact Center applies the first rule. If the email does not match that rule, Contact Center applies the next rule in the list. Contact Center continues to apply the rules in order, until the email matches a rule. If the email does not match any rule in the list, Contact Center creates the contact using the SN system default rule. You must make sure you place rules in the correct order to achieve the routing results that you want.

Use caution when you edit the SN system default rule, for the following reasons:

- If you change the properties of the rule, you affect the behavior of the social networking system default rule, which affects all SMM recipient mailboxes.
- If you delete the skillset associated with the default rule, Contact Center uses SN_Default_Skillset.
- If you delete SN_Default_Skillset, the system stops processing SMM emails.

Prerequisites for Social Network contact Configuration

- Assign one or more mailboxes to which Social Media Manager sends email messages to create Social Networking contacts. Each mailbox must not be used for any other Multimedia contact type.
- Test SMM to ensure that it sends email messages to the correct mailbox.

- Configure the route points for any skillset you want to assign to a rule for an SMM mailbox. For more information about configuring skillsets, see *Avaya Aura® Contact Center Client Administration*.

Configuring the Social Networking System Default Rule

Before you begin

- Configure the route points for the skillset you assign to the system default rule. For more information about configuring skillsets, see *Avaya Aura® Contact Center Client Administration*.
- Log on to the Contact Center Manager Administration application.

About this task

Update the Social Networking system default rule to ensure that every email arriving at a configured mailbox creates an SN contact with a valid skillset. Contact Center uses the SN system default rule for any SN contact that does not match the rules you create when you configure Social Networking mailboxes.

When you configure a recipient mailbox for Social Networking, Contact Center automatically includes the SN system default rule as the last regular rule in the list of rules for the recipient mailbox.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, from the **CCMM Servers** list, select your CCMM server.
3. Click **Launch Multimedia Client**.

   The CCMM Administration utility opens.
4. In the left column of the CCMM Administration utility, click **Social Networking**.
5. Click **General Settings**.
6. Under **System Default Rule**, from the **Skillset** list, select a Social Networking skillset name.
7. To change the priority, under **Priority**, select a different priority for contacts routed using the system default rule.
8. Click **Save**.

Configuring Social Networking channels

Before you begin

- Confirm the correct channel name on the SMM server.
- Log on to the Contact Center Manager Administration application.

About this task

Follow this procedure to create a new Social Networking channel in Contact Center. You can then use this channel to make routing decisions when you configure Social Networking mailboxes. The channels you create must exist in SMM.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, from the **CCMM Servers** list, select your CCMM server.
3. Click **Launch Multimedia Client**.

   The CCMM Administration utility opens.
4. In the left column of the CCMM Administration utility, click **Social Networking**.
5. Click **General Settings**.
6. Under **Available Channels**, click the plus sign (+).
7. In the **Channel Name** field, enter the name of the new channel. This must match the name of the channel on SMM.
8. In the **Description** field, type a descriptive name for the new channel.
9. Click **Save**.

Adding a new Social Networking language

Before you begin

- Confirm the language identifier on the SMM server.
- Log on to the Contact Center Manager Administration application.

About this task

Follow this procedure to create a new Social Networking language in Contact Center. You can use this language to make routing decisions when you configure Social Networking mailboxes. The language you create must already exist in SMM.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, from the **CCMM Servers** list, select your CCMM server.

3. Click **Launch Multimedia Client**.

   The CCMM Administration utility opens.
4. In the left column of the CCMM Administration utility, click **Social Networking**.
5. Click **General Settings**.
6. Under **Available Languages**, click the plus sign (+).
7. In the **Language Value** field, enter the identifier of the new language.

   The identifier you enter must match the identifier of the language on SMM.
8. In the **Description** field, type a descriptive name for the new language.
9. Click **Save**.

Configuring Social Networking mailboxes

Before you begin

- Assign one or more mailboxes to which Social Media Manager sends email messages to create Social Networking contacts. Each mailbox must not be used for any other Multimedia contact type.
- Test SMM to ensure that it sends email messages to the correct mailbox.
- Configure the route points for any skillset you assign to a rule for this SMM mailbox. For more information about configuring skillsets, see *Avaya Aura® Contact Center Client Administration*.
- Log on to the Contact Center Manager Administration application.

About this task

Follow this procedure to configure a mailbox from which Contact Center can process Social Networking contacts, and to define rules by which Contact Center queues the SN contacts to skillsets.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, from the **CCMM Servers** list, select your CCMM server.
3. Click **Launch Multimedia Client**.

   The CCMM Administration utility opens.
4. In the left column of the CCMM Administration utility, click **Social Networking**.
5. Click **Mailbox Configuration**.
6. On the **Edit Social Networking Mailbox Configuration** screen, click **Add**.
7. In the **Edit Mailbox** section, on the **Mailbox** tab, enter the IP address of the mail server in the **POP3 Server** field.

8. In the **Mailbox** field, enter the name of the mailbox to which SMM sends the Social Networking contact emails.
9. In the **Domain** field, enter the domain of the mailbox you specified in the **Mailbox** field.
10. In the **Password** field, enter the password for the mailbox you specified in the **Mailbox** field.
11. In the **Confirm Password** field, enter the password again.
12. Click **Routing**.
13. On the **Routing** tab, click the **Add New Rule** button (+) to add a rule to this mailbox.
14. In the **Language** field, select the language of the SMM email messages that you want this rule to select.
15. In the **Sentiment** field, enter the sentiment of the SMM email messages that you want this rule to select.
16. In the **Channel** field, enter the channel of the SMM email messages that you want this rule to select.
17. In the **Minimum Relevance** field, enter the lowest relevance value of the SMM email messages that you want this rule to select.
18. In the **Skillset** field, enter the skillset to which you want Contact Center to assign Social Networking contacts created from emails that match this rule.
19. In the **Priority** field, enter the priority at which you want Contact Center to queue Social Networking contacts created from emails that match this rule.
20. Click **Add**.

    Contact Center adds the rule to the list.
21. If there is more than one rule on this mailbox, use the **Move This Rule Up in Sequence** and **Move This Rule Down in Sequence** buttons to set the relative order of the new rule.
22. Complete steps 11 to 19 for each rule that you want to add to this mailbox.

Variable definitions

Name	Description
Inbound Server	The name or IP address of the email server that hosts the mailbox to which SMM sends Social Networking emails.
Mailbox	The name of the mailbox, configured in SMM, to which SMM sends emails from which Contact Center creates SN contacts. You must use this mailbox only for SMM emails, because Contact

Table continues…

Name	Description
	Center routes all emails in this mailbox as SN contacts.
Domain	The domain name of the email server that hosts the mailbox.
Password	The password for the mailbox.
Confirm Password	The password for the mailbox, to confirm that you entered it correctly.
Language	The language, set by SMM that Contact Center checks on the SMM email to determine the routing of the SN contact.
Sentiment	The sentiment, set by SMM that Contact Center checks on the SMM email to determine the routing of the SN contact.
Channel	The channel (social media source), set by SMM that Contact Center checks on the SMM email to determine the routing of the SN contact.
Relevance	The relevance, set by SMM that Contact Center checks on the SMM email to determine the routing of the SN contact.
Skillset	The skillset to which Contact Center assigns this contact, if it meets all the criteria you configured in the Rule Output section. If a contact does not meet all the criteria, Contact Center does not implement this rule.
Priority	The priority at which Contact Center queues this contact, if it meets all the criteria you configured in the Rule Output section.

Configuring mailboxes for transferred Social Networking contacts

Before you begin

- Configure one or more Social Networking mailboxes.

About this task

Configure mailboxes from which Contact Center sends SN contacts that agents transfer out of the contact center.

When an agent transfers a Social Networking contact to someone who is not a Contact Center agent, Contact Center sends the contact as an email. For each skillset, you can select the mailbox from which Contact Center sends transferred contacts. You must configure as a Social Networking mailbox each mailbox you want to use for transferring SN contacts.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, from the **CCMM Servers** list, select your CCMM server.
3. Click **Launch Multimedia Client**.

   The CCMM Administration utility opens.
4. In the left column of the CCMM Administration utility, click **Social Networking**.
5. Click **Transfer Configuration**.
6. Under **Social Networking Transfer Configuration**, from the **Skillset** list, select a Social Networking skillset name.
7. In the corresponding **E-mail Address** field, select a Social Networking mailbox from which contact center can send transferred contacts for the skillset.

   Only Social Networking mailboxes appear in the drop-down list.
8. Click **Save**.

Chapter 30: Instant message configuration

The Contact Center Multimedia server supports text-based conversations between the customer and the agent in a SIP-based environment using Instant Messaging. Customers initiate an instant message contact and choose from a list of skillsets to pick the appropriate topic for the contact.

To personalize the Web communications contacts, you can configure welcome messages for all contacts and specialized messages for each skillset. You can also configure disconnect messages.

To assist agents with instant message contacts, you can use automatic phrases to configure text for agents to automatically insert in the text-based conversation. You can also configure page push URLs, a predefined URL that is commonly sent to customers. The automatic phrases and page push URLs save the agent typing time when communicating with the customer.

Note:

Instant message configuration procedures do not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Configuring welcome and disconnect messages

About this task

Create a custom welcome and disconnect message for the contact center or for individual skillsets.

The welcome and disconnect messages for an instant message contact have a message to welcome customers who initiate the contact and a message to indicate when the contact is complete.

The customer sees only one welcome or disconnect message. If you configure a welcome or a disconnect message for a skillset, the skillset message appears. If you configure the default welcome or disconnect message and not a skillset message, the customer sees only the default message.

Procedure

1. Open the Multimedia Administration utility.
2. In the left pane, click **IM**.
3. Click **Resources**.

4. In the **Welcome Message** box, type the message to appear at the beginning of every contact. The maximum size for this message is 255 characters.
5. In the **Disconnect Message** box, type the text to appear at the end of the contact when the agent disconnects.
6. To create a customer welcome message for a specific skillset, under **Custom Welcome Messages**, select a skillset.
7. Under **Welcome Message**, type the welcome message for the selected skillset.
8. Under **Disconnect Message**, type the disconnect message for the selected skillset.
9. Click **Save**.

Creating automatic phrases

About this task

Create automatic phrases by skillset. You can create a list of commonly used phrases for agents to insert into their instant message contacts instead of typing individual responses.

You can select an automatic phrase for all skillsets. If you choose all skillsets, the phrase applies to all skillsets for Web communications and instant message contacts.

Procedure

1. Open the Multimedia Administration utility.
2. In the left pane, click **IM**.
3. Click **Auto Phrases**.
4. Under **Edit Auto Phrases**, select the skillset to add new phrases.

   OR

   Click **All Skillsets** to apply an automatic phrase for all skillsets.
5. Click **Edit**.
6. In the **Previously Configured Auto Phrase** box, review the phrase to determine whether to change it or use it for other skillsets.

   Important:

   If you select **All Skillsets**, the **Previously Configured Auto Phrase** box is unavailable.
7. In the **Name** box, type a name to represent this automatic phrase.
8. In the **Phrase Text** box, type the text that is commonly used for the contacts based on the selected skillset.
9. Click **Add**.

10. Click **Save**.

Creating a page push URL

About this task

In the Agent Desktop, the agent can choose from a list of Web pages specified for the skillset assigned to the instant message contact.

Create the Web pages that appear the Agent Desktop. Ensure that you make the name of the page push URL descriptive to assist the agents using the Agent Desktop.

You can configure maximum 50 URLs.

Procedure

1. Open the Multimedia Administration utility.
2. In the left pane, click **IM**.
3. Click **Page Push URLs**.
4. Under **Edit Page Push URLs**, select the skillset to add new URLs.

   OR

   Select **All Skillsets**.
5. Click **Edit**.

   The Edit Push Page URL dialog box appears.
6. In the **URL** box, type the URL for the website to add to the list that appears in the Agent Desktop.
7. In the **Description** box, type a description for the page push URL that describes the URL that the agent can push.
8. Click **Add**.
9. Click **Save**.

Adding an expert manually to Contact Center Multimedia

About this task

To add an agent to the Experts list, you can manually add an agent to CCMM.

Procedure

1. Open the Multimedia Administration utility.

2. In the left pane, click **IM**.
3. Click **Import Experts**.
4. Click the **Manual** tab.
5. In the **Name** box, type the name of the expert.
6. In the **URI** box, type the URI of the expert.
7. Optional: In the **Custom 1** and **Custom 2** boxes, type the custom information of the user as required.
8. Optional: In the **Phone** box, type the extension of the expert.
9. Click **Add**.

Importing an expert from files to Contact Center Multimedia

About this task

To add an agent to the Experts list, you can import an expert from files to CCMM.

Procedure

1. Open the Multimedia Administration utility.
2. In the left pane, click **IM**.
3. Click **Import Experts**.
4. Click the **File Import** tab.
5. In the **File Name** box, type the complete path for the file.

   OR

   Click **Browse** to browse to the file.
6. Select the delimiter for the values.
7. Click **Next**.
8. Select **First Row contains column headers**, to indicate that the first row of data in the file are column names.
9. Click **Next**
10. Select the columns that correspond to the Expert fields. The **Name** and **URI** fields are mandatory.

Adding experts to a skillset

Before you begin

- Skillsets must be configured.

About this task

You can add experts to a skillset associated group.

Procedure

1. Open the Multimedia Administration utility.
2. In the left pane, click **IM**.
3. Click **Skillset Experts**.
4. Select the skillset from the list and click **Edit**.
5. Select the experts you want to add to the skillset from the **Skillset Experts** list.
6. Click **Skillsets**.
7. Select the expert and click **>** to add the experts to the skillset.
8. Click **Save**.

Creating an expert group

Before you begin

- Ensure that you have agent names in the Experts list.

Important:

If the group name begins with an '_' (underscore), then this group is an Always-on group. An Always-on group is always present in the list of contacts in the CC Contacts tab in the Presence control, on the Agent Desktop.

About this task

After you create an experts group, agents in your contact center can consult Instant Experts groups after they log on to Agent Desktop.

Procedure

1. Open the Multimedia Administration utility.
2. In the left pane, click **IM**.
3. Click **Expert Groups**.
4. Click **New**.
5. In the **Name** box, enter a name for the group.

6. In the **Keyword** box, enter a keyword for the group.
7. Click **>**.
8. Repeat step 6 for any keywords you want to associate with the group.
9. Select any keywords you want to remove and click **Remove**.
10. Click **New**.
11. Select the experts you want to add from the **Expert Group** list.
12. Click **>** to add the experts to the skillset.
13. To remove an expert, select the expert, and click **<**.
14. Click **OK**.

Variable definitions

Name	Description
group name	There are three types of Instant Experts groups: • Groups that automatically display after an agent logs on to Agent Desktop. These group names begin with an underscore (_), for example, _autoload. • Groups that automatically display with associated skillsets. • Groups that display after an agent clicks on a highlighted keyword in a text chat with a contact.

Chapter 31: Short Message Service configuration

This chapter contains the configuration steps for the SMS recipient mailbox.

In the contact center, the recipient mailboxes are polled for incoming Short Message Service (SMS) messages. A server forwards the SMS messages to an email address. The Contact Center Multimedia Email Manager retrieves the text of the SMS and queues it to the appropriate skillset with an assigned priority. The caller ID is extracted to facilitate callbacks to the customer.

Reports appear in the Contact Center Multimedia Administration utility to show the current traffic status. The following reports appear when you select Text Messages (SMS) and View Reports in the left column of the Contact Center Multimedia application. You can choose the report date and the skillsets represented in all displayed real-time reports.

- The SMS (New Vs. Closed) report shows the number of contacts in a new and closed state against the time for the selected date and skillsets.
- The SMS Progress report shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for that date.
- The SMS Closed Contacts Queue Time report shows the average time a contact spends in queue while the contact center is open.

Note:

Short Message Service configuration procedures do not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Prerequisites for SMS configuration

Procedure

Ensure that you are licensed for email contacts.

Configuring a route point for an SMS skillset

About this task

Configure a route point for an SMS skillset to route SMS contacts to an agent. Skillsets are used to assign the contacts to agents.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **General Administration**.
3. Click **Skillset Settings**.
4. In the **Skillset Settings** dialog box, select the skillset to assign a route point.

   The skillset must have the prefix SM.
5. Under the **Edit Skillset** dialog box, in the **Route Point** list, select the route point to assign to the SMS skillset.
6. Click **Save**.

Variable definitions

Name	Description
Route point	A location in the open queue that enables incoming contacts to queue and run through a script on the Contact Center Manager Server.

Adding an SMS Gateway

About this task

Add the SMS server for your Contact Center Multimedia server as per your requirement.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Click **SMS Gateway** (image).
5. In the SMS Gateway Configuration window, click **Add**.

6. In the **SMS Gateway** box, type the name of the new server.
7. Click **Save**.

Updating an SMS Gateway

About this task

Update the SMS server for your Contact Center Multimedia server as per your requirement.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Click **SMS Gateway** (image).
5. In the SMS Gateway Configuration window, click **Edit**.
6. Change the properties of your SMS server.
7. Click **Save**.

Deleting an SMS Gateway

About this task

Delete the SMS server for your Contact Center Multimedia server if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Click **SMS Gateway** (image).
5. In the SMS Gateway Configuration window, select the SMS gateway you are deleting and click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.
7. Click **Close**.

Adding a SMS mailbox

Before you begin

- Configure a skillset for a SMS contact.

About this task

Add a SMS mailbox to the multimedia configuration for receiving SMS messages in an email message.

Also, choose the skillset for the mailbox so that the SMS message is routed to the agent who has the optimal skillset to handle the specific contact.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Click **Add**.
5. On the **Mailbox** tab, in the **Inbound Server** field, select the host name of your POP3 or IMAP server along with the respective security protocol.
6. In the **Outbound Server** field, select the host name of your SMTP server.
7. In the **Mailbox** field, type the mailbox name.
8. In the **Domain** field, type the mailbox domain.
9. In the **Password** and **Confirm** fields, type and retype the password to access the mailbox.
10. In the **Skillset** field, choose a configured skillset for routing the contacts.
11. In the **Contact Priority** field, choose a priority for contacts received in this mailbox.
12. Click the **Sender Address** tab.
13. Select **Use full sender address** or **Parse sender address for CLID**.
14. If you select **Parse sender address for CLID**, in the **Leading Characters to Remove** field, type the characters that you must not dial when making the outgoing callback.
15. Click **Save**.

Variable definitions

Name	Description
Inbound Server	The host name of the email server that handles email messages entering the contact center.

Table continues…

Name	Description
Outbound Server	The host name of the email server that delivers email messages that leave the contact center.
Mailbox	Name of the mailbox on the email server that is polled for new incoming email messages.
Domain	The domain name for the email server.
Password	The password used to access the mailbox on the email server. Type the password in the Confirm Password box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.
Skillset	A label applied to a set of skills, capabilities, or knowledge that an agent requires to respond to a request. The skillsets are retrieved from the Contact Center Manager Server database. You must select a route point for a skillset used to route SMS contacts.
Priority	The priority given to a request for a skillset agent. The lower the priority number, the greater the priority. The values of the priorities range from 1 to 6. For example, a call with priority 1 is handled before a call with priority 6.
Sender address	Select Use full sender address or Parse the address for the Calling Line identification (CLID) to save for future contacts. The address in the format you select is stored with the contact for future communication with the customer.
Leading characters to remove	If you select Calling Line Identification (CLID) to add the customer's phone number into the contact information, type any leading characters or trunk numbers to remove from the current number.

Updating an SMS mailbox

Before you begin

- Add an SMS mailbox.

About this task

Update the properties of the SMS mailbox, as per your requirements.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be edited.
5. Click **Edit**.
6. Update the mailbox settings as required.
7. Click **Save**.

Deleting an SMS mailbox

Before you begin

- Add an SMS mailbox.

Important:

An SMS mailbox cannot be deleted if it is currently assigned to a skillset.

About this task

Delete an SMS mailbox, if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Configuring an SMS reply mailbox

About this task

Configure the reply information for the SMS message received by your contact center.

Configure the outgoing mailbox properties with a signature related to the skillset for replying to an SMS.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Text Messaging (SMS)**.
3. Click **Reply Configuration**.
4. Under **Skillsets**, select a fax skillset for the mailbox configuration.
5. Under **Mailbox**, select a configured mailbox.

   OR

   Click **New** to create a new mailbox.

   OR

   Click **Edit** to edit an existing mailbox.
6. In the **SMTP Server** box, select the SMTP server to use for outgoing email messages.
7. In the **Mailbox** box, specify the new mailbox or change the name of the existing mailbox.
8. In the **Domain** box, type the email server domain.
9. In the **Password** and **Confirm** boxes, type the email server password.
10. To use a different user name for the SMTP authentication, select the **Use Alternative username for SMTP Authentication** check box.
11. In the **Username** box, type the alternative user name.
12. Click **Save**.

Variable definitions

Name	Description
SMTP Server	The name of the email server that handles email messages leaving the contact center.
Mailbox	Name of the mailbox on the email server polled for email messages.
Domain	The domain name for the email server.
Password	The password used to access the mailbox on the email server. Type the password in the Confirm Password box to ensure accuracy. Contact Center Multimedia supports a maximum mailbox password length of 100 characters.

Table continues…

Name	Description
Use Alternative username for SMTP Authentication	If SMTP authentication is required for your outbound email server, select the user name for the authentication.

Deleting an SMS reply mailbox

About this task

Delete an SMS reply mailbox, if it is no longer required.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Text Messaging (SMS)**.
3. Click **Reply Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Updating the SMS system default rule

Before you begin

- Ensure that you know the default settings for the system delivery failure rule:
  - use the SMS default skillset, SM_Default_Skillset
  - use no automatic response
  - assign priority 3
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, SM_Default_Skillset is used.
- Configure the route points for the skillset you assign to the system default rule. For more information, see Configuring a route point for an SMS skillset on page 333.

About this task

Update the SMS system default rule to ensure that email messages received with SMS text are routed to an agent if no other rule associated to the recipient mailbox routes the email message.

The system default rule is used in every rule group configured in Contact Center Multimedia.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Text Messaging (SMS)**.
3. Click **Default Rules**.
4. Under **System Default Rule**, from the **Skillset** list, select a skillset name to assign to the contact.
5. Under **System Default Rule**, from the **Priority** list, select the priority to assign to the contact.
6. Click **Save**.

Updating the SMS system delivery failure rule

Before you begin

- Ensure that you are licensed to handle email messages.
- Ensure that you know the default settings for the system delivery failure rule:
  - use the SMS default skillset, SM_Default _Skillset
  - use keyword group delivery failure keywords
  - assign priority 10 (lowest)
- Use caution when you change the properties of the system default rule:
  - If you change the properties of the rule, you affect the behavior of the system default rule, which affects all recipient mailboxes.
  - If you delete the skillset associated with the default rule, SM_Default_Skillset is used.
- Configure the route point for the skillset you plan to assign to the system delivery failure rule. See Configuring a route point for an SMS skillset on page 333.

About this task

Update the SMS system delivery failure rule to ensure that any email message that contains particular phrases such as undeliverable, returned mail, unknown recipient, delivery failure, or delivery report is deleted, and not assigned to an agent.

When you create a recipient mailbox, the system delivery failure rule is copied as the first regular rule into list of rules for the recipient mailbox.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Text Messaging (SMS)**.
3. Under **System Delivery Failure Rule**, from the **Skillset** list, select a skillset name to assign to the contact.
4. To change the keyword group, select the keyword group which contains the delivery failure keywords from the **Keyword Group** list under the **System Delivery Failure Rule**.
5. To change the priority, under **Priority**, select the priority to assign to the contact from the **Priority** list under the **System Delivery Failure Rule**.
6. To close contacts matching the delivery failure keywords, select the **Will close contact** check box.
7. Click **Save**.

Chapter 32: Web communications configuration

The Contact Center Multimedia server supports text-based conversations between the customer and the agent by using Web communications text chat or Enterprise Web Chat (EWC). When customers initiate a Web communications contact, a list of skillsets determines the appropriate topic for the contact.

EWC supports integration with Agent Desktop only with a standalone Multimedia server on a Unified Communications solution. EWC is a licensed feature, and requires a Web Chat SDK license.

Note:

If you are migrating from an existing Web Communications chat solution to the EWC chat solution, you must redevelop your custom interfaces to integrate with EWC.

Contact Center selects EWC as the web chat solution, if the following criteria are satisfied:

1. Agent have logged on to Agent Desktop.
2. Agents are assigned to a skillset for handling web communications.
3. Contact Center is licensed for EWC.

Before making any Web communications contacts, you must ensure the Web communications server or Enterprise Web Chat server is configured.

Note:

Agent Desktop handling of web communications contacts is the same whether Contact Center uses Web Communications chat or EWC. You must enable Agent Desktop to handle EWC contacts using the CCMM Administration utility. By default the option is not enabled. You can enable the option only if your Contact Center has the EWC license.

To personalize the Web communications contacts, you can configure welcome messages for all contacts, and specialized messages for each skillset. You can place labels in the text-based conversation to identify the text written by the customer and agent. You can also send a copy of the transcript of the Web communication contact to the customer when the contact is complete.

Timers control the length of time for alerts to indicate when the agent or customer stops responding in the Web communication contact.

To assist agents with Web communications contacts, you can use automatic phrases to configure text for agents to automatically insert in the text-based conversation. You can also configure page

push URLs, predefined URLs that are commonly sent to customers. The automatic phrases and page push URLs save the agent typing time when communicating with the customer.

The Web on hold URLs create a list of Web pages that are sent to the customer’s desktop while they wait for an agent to respond to their initial contact.

A Web on hold comfort group creates a list of messages that are sent to the customer’s desktop, while the customer waits for an agent to respond, for a specified period of time to their initial contact, on a Web communications skillset.

A Web communications comfort group creates a list of messages that are sent to the customer's desktop while they wait for an agent to respond, for a specified period of time, either to their initial contact or during the communication, on a Web communications skillset.

An agent-supervisor can observe or participate in any currently active agent-customer Web communications chat session, provided the agent is under the supervision of that particular agent-supervisor. Agent-supervisors using Avaya Agent Desktop can see a display of all such applicable Web communications and Voice contacts currently active. This display also flags any Web communications contacts where certain intrinsic values exceed the defined threshold. If Contact Center uses the EWC chat solution then an agent-supervisor can send whisper messages to the agent. Whisper messages are not seen by the customer. Whisper messages are not supported in the Web Communications chat solution.

Note:

Web communications configuration procedures do not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Prerequisites for Web communications configuration

Procedure

- Ensure that you have a license for Web communications.
- Additionally, if you are using Enterprise Web Chat (EWC), ensure that you have an EWC feature license.

Assigning a development Web server name

Before you begin

- Know the name of your development Web server and the production Web server.

About this task

Configure the external Web server name to identify the external Web server for Web contacts received by the contact center.

If you configured the external Web server during installation, and the name of the server remains the same, you can skip this procedure. If you move your external website from a test computer to the production server, you must configure the external Web server name.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **General Administration**.
3. Click **Server Settings**.
4. In the **Server Settings** dialog box, select **External Web Server** and click **New**.
5. In the **Server Name** box, type the name of the external Web server where you plan to install the sample Web customer interface and develop your custom website.
6. In the **Server Port** box, type the port number for the external Web server you use to develop your custom website.
7. Click **Save**.

Variable definitions

Name	Description
Server Name	The name of the external Web server on which you plan to install the sample Web customer interface and develop your custom website.
Server Port	The port number for the external Web server for your custom website.

Configuring welcome messages and text chat labels

About this task

The welcome messages and text chat labels for a Web communications contacts have a welcome message for customers who initiate the contact, and labels for the agent and customers in the text conversation.

Configure a default welcome message that appears for all skillsets and welcome messages that apply for a single skillset. One welcome message appears for the customer. If the welcome message for the skillset appears, the global welcome message does not. The customer chooses the skillset when they initiate the contact.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.

2. In the left pane, click **Web Comms**.
3. Click **Resources**.
4. In the **Default Welcome Message** box, type the message to appear at the beginning of every contact. The maximum size for this message is 255 characters.
5. In the **Agent Label** list, select the label to appear at the beginning of the agent contact list.

   In the first box, choose from a list of automatic text such as Friendly Name, First Name, Last Name, or both First Name and Last Name. Use the second box to type custom text.
6. In the **Customer Label** box, type the text to appear at the beginning of the customer responses in the contact.

   Note:

   Customer Label is supported up to version xampp-win32-1.7.2 only.
7. To create a customer welcome message for a specific skillset, under **Custom Welcome Messages**, select a skillset.
8. Under **Welcome Message**, type the welcome message for the skillset.
9. Click **Save**.

Variable definitions

Name	Description
Agent Label	The label that appears beside the text typed for the agent. Select one of the following items: • First Name: The first name of the agent appears at the beginning of the agent responses in the contact (for example, Robert). • First Name, Last Name: The first and last name of the agent appear at the beginning of the agent responses in the contact (for example, Robert Smith). • Last Name, First Name: The last name of the agent, followed by the first name of the agent appears at the beginning of the agent responses in the contact (for example, Smith, Robert). • Friendly Name: The friendly name or nickname of the agent appears at the beginning of the agent responses in the contact (for example, Rob). The first name of the agent is the default value for Friendly Name. For example, if you have entered the first name of the agent as Fred in Contact Center Manager Administration, the default

Table continues…

Name	Description
	Friendly Name is set as Fred. You can modify the Friendly name using Contact Center Multimedia. While upgrading to Contact Center 7.0.1, the default value is applied to any existing agents. The default values is also applied to any new agents who are added to the system after the upgrade. You can also type custom text to appear at the beginning of the agent responses. The maximum size of the label is 255 characters.
Customer Label	The text to appear at the beginning of the customer responses in the contact. The maximum size of the Customer Label is 255 characters.

Configuring Enterprise Web Chat settings

Before you begin

Enterprise Web Chat (EWC) works only if Avaya Aura® Contact Center is deployed on Communication Manager with a standalone Multimedia server and your Contact Center is licensed for EWC.

About this task

Configure the EWC server domain and optionally the Transcript Filtering Web Service, if your Contact Center uses Enterprise Web Chat (EWC).

Use the Transcript Filtering Web Service to modify EWC chat transcripts before the transcripts are saved to the Multimedia database. Creating filters is the responsibility of the customers and a sample filter is provided as part of the EWC SDK. You can configure EWC to use a transcript filter created by the customer. The transcript filter can be used to modify the transcript to mask sensitive data such as account details, credit card numbers, or personal identification numbers. The transcripts are associated with the customer record whose email sent the chat request.

Note:

EWC filters out the < and > characters making these characters invisible to the other party in the chat. Therefore, in EWC chat messages, agents or customers must not use the < or > characters.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Config**.

4. To enable your Agent Desktop to handle EWC contacts, click the **Enable Enterprise Web Chat** option.

   By default the **Enable Enterprise Web Chat** option is not enabled. You can select the **Enable Enterprise Web Chat** option only if the EWC license is present.

5. In the **External Web Server Domain** box, type the domain name for the server hosting the customer-facing website for EWC.

6. **(Optional)** In the **Transcript Filtering Web Service** box, type the URL of a REST service used to filter customer chat transcripts.

   The format of the URL of the REST service is either `http://<uri>` or `https://<uri>`, where `<uri>` is the service URI of the transcript filtering service.

   For more information on Transcript Filtering Web Service, see the SDK documentation.

7. Click **Save**.

Configuring skillsets for Web Communications

Before you begin

- Configure comfort messages, Web on Hold comfort groups and URLs, or chat history header responses that you want to use on your Web Communications skillsets. For more information, see Configuring Web communications comfort groups for a Web communications skillset on page 234, Configuring Web On Hold comfort groups for a Web communications skillset on page 232, and Creating or changing prepared responses on page 258.

About this task

Configure a route point for a skillset to use the skillset for routing contacts. A route point is a location on the open queue that enables incoming calls to be queued and run through a script on the Contact Center Manager Server.

You can apply comfort messages, Web On Hold comfort groups and URLs, and chat history headers to Web Communications skillsets. You cannot set an auto-signature on a Web Communications skillset.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **General Administration**.
3. Click **Skillset Settings**.
4. Select a WC skillset from the list.
5. In the **Edit Skillset** section, from the **Route Point** list, select the route point to assign to the skillset.

6. Optionally, under **Chat History Header**, choose a chat history header response to include in email messages that Contact Center Multimedia sends to customers with their chat history.
7. Optionally, under **Comfort Group**, choose a group of comfort messages to display to customers who are queued on this skillset.
8. Optionally, under **On Hold Group**, choose a group of comfort messages to display to customers who an agent has put on hold.
9. Optionally, under **Web On Hold Group**, choose a group of on hold URLs to display to customers who an agent has put on hold.
10. Click **Save**.

Configuring Web communications agent timers

About this task

Configure the contact timers for Web communications conversations in your Contact Center.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Config**.
4. In the **Keep Alive Time** box, type the interval in minutes and seconds between heartbeat pulses that verify whether both ends of the Web communications contact are open.
5. In the **Message Refresh** box, type the refresh time for the Agent Desktop.
6. In the **Desirable Response (Customer awaiting Agent)** box, type the threshold for the agent to respond.
7. In the **Desirable Response (Agent awaiting Customer)** box, type the threshold for the customer to respond.
8. In the **Consult Request Timeout** box, type the length of time in seconds that a consultation is requested before it times out.
9. Select the **Force Idle Customer Check** check box so that the Agent Desktop alerts agents when a customer has not replied in a Web communications session, for a predefined period. The Agent Desktop also brings that web chat contact to the front.
10. In the **Force Idle Customer Check Timeout** box, type the time after which the Agent Desktop considers a customer in a web chat session idle, if a customer has not responded in a Web communications session.
11. Click **Save**.

Variable definitions

Name	Description
Message Refresh	The refresh time for the Agent Desktop.
Keep Alive Time	The interval in minutes and seconds between heartbeat pulses that verify whether both ends of the Web communication contact are open.
Desirable Response (Agent awaiting Customer)	The time after which the conversation indicator on the Agent Desktop changes color to indicate that the desirable time for an agent response is exceeded.
Desirable Response (Customer awaiting Agent)	The time after which the conversation indicator on the Agent Desktop changes color to indicate that the desirable time for a customer response is exceeded.
Consult Request Timeout	The time after which the consult request expires.
Force Idle Customer Check	Select this check box to enable Agent Desktop to alert agents when a customer has not replied in a Web communications session, for a predefined period. The Agent Desktop also brings that web chat contact to the front.
Force Idle Customer Check Timer	The time after which the Agent Desktop considers a customer in a web chat session idle, if a customer has not responded in a Web communications session.

Saving Web communications chat session details

About this task

Configure the details you want to save for each Web communications chat session in your contact center.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Config**.
4. Select the **Save Timestamp on Chat Message** check box to enable the saving of a time-stamp with each chat message sent in a chat session.

5. Select the **Save Chat History** check box to enable the saving of chat session history. When enabled, the entire history of a chat session is saved.

   Important:

   The **Save Timestamp on Chat Message** and **Save Chat History** settings are not applicable to the Enterprise Web Chat (EWC) chat solution. Use the EWC Transcript Filtering Web Service feature to modify the EWC chat transcripts. See Configuring Enterprise Web Chat settings on page 346.

6. Click **Save**.

Configuring the Web communications chat session limits

About this task

Configure limits for Web communications chat sessions. These limits restrict the number of concurrent sessions and scheduled callbacks that a customer can have. Setting these limits reduces the possibility of Denial of Service attacks through the Web communications interface.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Config**.
4. In the **Concurrent Chats Limit per Customer** box, type the maximum number of concurrent chat sessions each customer can create. Type a value between 1 and 10. The default value is 3, which is the value that Avaya recommends.
5. In the **Requested Call-backs Limit per Customer** box, type the maximum number of scheduled Web communication callbacks each customer can have. Type a value between 1 and 10. The default value is 3, which is the value that Avaya recommends.
6. Click **Save**.

Configuring customer notification log

Before you begin

- Configure an outgoing email address to use to send the log file to the customer.

About this task

Configure the customer notification log information to prepare to send an email to the customer of the written conversation.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Config**.
4. Under **Chat Conversation**, select **E-mail Chat Log to Customer**.
5. Click **Save**.

Enabling Web Communications transfer to a skillset

About this task

Configure the Web Communications (WC) transfer to a skillset feature to allow agents to transfer a WC contact to a skillset.

Note:

If you want to transfer a Web Communications contact, your contact center must be licensed to use the Multiplicity feature.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Config**.
4. Select the **Enable Transfer To Skillset** checkbox.
5. Click **Save**.

Creating automatic phrases

About this task

Configure automatic phrases by skillset. You can create a list of commonly used phrases for agents to insert into their Web communications contacts instead of typing individual responses.

You can select a single automatic phrase for all skillsets. If you choose all skillsets, the automatic phrase applies to all skillsets for Web communications and instant message contacts.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Auto Phrases**.
4. Under **Edit Auto Phrases**, select the skillset to add new phrases.

   OR

   Click **All Skillsets** to apply an automatic phrase for all skillsets.
5. Click **Edit**.
6. In the **Previously Configured Auto Phrase** box, review the phrase to decide whether you want to change it or to use it for other skillsets.

   Important:

   If you select All Skillsets, the Previously Configured Auto Phrase box is unavailable.
7. In the **Name** box, type a name to represent this automatic phrase.
8. In the **Phrase Text** box, type the text that is commonly used for the contacts based on the selected skillset.
9. Click **Add**.
10. Click **Save**.

Deleting an automatic phrase

About this task

Delete the automatic phrase to remove it from the list of automatic phrases available to the agents in the Agent Desktop.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Auto Phrases**.
4. Under **Edit Auto Phrases**, select the skillset from which you want to remove the phrases.

   OR

   Select **All Skillsets** to remove phrases for use with all skillsets.
5. Click **Edit**.

6. In the **Phrases in Group** box, select the automatic phrase to delete.
7. Click **Remove**.

   The system displays a Warning dialog box.
8. Click **Yes** to confirm the decision.
9. Click **Save**.

Creating a page push URL

About this task

In the Agent Desktop, the agent can choose from a list of Web pages for the skillset assigned to the Web communication contact.

Create the Web pages that appear the Agent Desktop. Ensure that the name of the page push URL is descriptive to assist agents in using the Agent Desktop.

You can configure maximum 50 URLs.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Page Push Urls**.
4. Under **Edit Page Push URLs**, select the skillset to add new URLs.

   OR

   Select **All Skillsets**.
5. Click **Edit**.
6. In the **URL** box, type the URL for the website to add to the list that appears in the Agent Desktop.
7. In the **Description** box, type a description for the page push URL that describes the URL that the agent can push.
8. Click **Add**.
9. Click **Save**.

Deleting a page push URL

About this task

Delete a page push URL to remove it from the list of pages the agent can push to customers during a Web communications contact.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Page Push Urls**.
4. Under **Edit Page Push URLs**, select the skillset to change the URLs.

   OR

   Select **All Skillsets**.
5. Click **Edit**.
6. In the **URLs in Group** box, select the URL to delete.
7. Click **Remove**.

   The system displays a Warning dialog box.
8. Click **Yes** to confirm the decision.
9. Click **Save**.

Creating Web On Hold URLs groups

About this task

Web On Hold URL groups is a sequence of URLs presented automatically to a customer's Web browser while the customer waits for an agent in the Web communications. You can define the time that each URL appears on the customer's Web browser.

Web On Hold URLs can include multimedia formats, such as video clips (Quick Time) or audio files (MPEG3). However, the customer browser must be able to play these formats. Customers are responsible for the plug-ins needed to run multimedia files.

You can add up to 50 URLs to a Web-on-hold group, but Avaya recommends that you use no more than 25 URLs in each Web-on-hold group.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.

3. Click **Web On Hold**.
4. Click the **On Hold URLs** tab.
5. Click **New**
6. In the **Tag** box, type a name for the new Web On Hold group.
7. In the **Description** box, type a description for the Web On Hold URL.
8. In the **Hold Time** box, type the number of seconds to display each URL in the customer's browser.
9. In the **URL** box, type the URL to display on the customer's Web browser.
10. Click **Add**.
11. Repeat step 6 on page 355 to step 11 on page 355 to add all URLs to the current Web on hold group.
12. Click **Save**.

Deleting a URL from a Web On Hold URL group

About this task

Delete a URL from a Web on hold URL group if the URL is not available.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Web On Hold**.
4. Click the **On Hold Urls** tab.
5. Click **Edit**.
6. Under **Edit Web On Hold URL Group** dialog box, in the **URLs in Group** box, select the URL to delete.
7. Click **Remove**.

   The system displays a Warning dialog box.
8. Click **Yes** to confirm the decision.
9. Click **Save**.

Deleting a Web On Hold URLs group

About this task

Delete a Web-on-hold URLs group to avoid displaying the Web pages to the customer during Web communications contacts.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Web On Hold**.
4. Click the **On Hold Urls** tab.
5. Select the **Group** to delete.
6. Click **Delete**.

   The system displays a Warning dialog box.
7. Click **Yes** to confirm the deletion.

Creating Web On Hold comfort groups

Before you begin

- Add the Web on hold comfort group to the Web communications skillset. For more information adding comfort groups to a Web communications skillset, see Configuring Web On Hold comfort groups for a Web communications skillset on page 232.

About this task

A Web on hold comfort group consists of a list of sequential messages that are sent to the customer's desktop, while the customer waits for an agent to respond, for a specified period of time to their initial contact, on a Web communications skillset. You can also add variables to the Web on hold message text for a customer.

You can set the time for which messages display on the customer's desktop.

Note:

Avaya recommends that you use no more than five messages in each Web on hold comfort group and one Web on hold comfort group for each Web communications skillset.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.

3. Click **Web On Hold**.
4. Click the **On Hold Comforts Group** tab.
5. Under **Comfort Group**, click **New**.
6. In the **Name** box, type a name for a new Web on hold comfort group.
7. In the **Delay** box, type the number of seconds to display each comfort message in the customer's desktop.
8. In the **Message** box, type the comfort message.
9. Optional: To insert a placeholder for accessing variables for the message, right-click in the **Message** box and select the placeholder from the menu.
10. Click **Add**.
11. Repeat step 9 and step 10 to add messages to the current Web on hold comfort group.
12. Under **Group Messages**, use the arrow keys to configure the sequence of messages.
13. Click **Save**.

Deleting a message from a Web On Hold comfort group

Before you begin

- Set up a Web on hold comfort group that is associated with Web communications skillset.

About this task

Follow this procedure to delete a comfort message from a Web on hold comfort group, if you do not want to use a specific message in the comfort group.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Web On Hold**.
4. Click the **On Hold Comfort Groups** tab.
5. Under **Comfort Group**, select the **Group** that contains the **Message** to delete.
6. Click **Edit**.
7. Under **Group Messages**, select the **Message** to delete.
8. Under **Edit Group**, click **Remove**.

   The system displays a Warning dialog box.
9. Click **Yes** to confirm the decision.

10. Click **Save**.

Deleting a Web On Hold comfort group

Before you begin

- Set up a Web on hold comfort group that is associated with Web communications skillset.
- Ensure that the Web on hold comfort group is unlinked from any other skillset before it is removed.

About this task

Follow this procedure to delete a Web on hold comfort group if you do not want to use a specific comfort group.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Web On Hold**.
4. Click the **On Hold Comfort Groups** tab.
5. Under **Comfort Group**, select the **Group** to delete.
6. Click **Delete**.

   The system displays a Warning dialog box.
7. Click **Yes** to confirm the deletion.

Creating Web communications comfort groups

Before you begin

- Add the Web communications comfort group to the Web communications skillset. For more information adding Web communications comfort groups to a Web communications skillset, see Configuring Web communications comfort groups for a Web communications skillset on page 234.

About this task

A Web communications comfort group consists of a list of sequential messages that are sent to the customer's desktop while they wait for an agent to respond, for a specified period of time, either to their initial contact or during the communication, on a Web communications skillset. You can also add variables to the Web communications message text for a customer.

You can set the time for which messages display on the customer’s desktop.

Note:

Avaya recommends that you use no more than five messages in each Web communications comfort group and one Web communications comfort group for each Web communications skillset.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Comfort Messages**.
4. Under **Comfort Group**, click **New**.
5. In the **Name** box, type a name for a comfort group.
6. In the **Delay** box, type the number of seconds to display each comfort message in the customer's desktop.
7. In the **Message** box, type the comfort message.
8. Optional: To insert a placeholder for accessing variables for the message, right-click in the **Message** box and select the placeholder from the menu.
9. Click **Add**.
10. Repeat step 8 on page 359 and step 9 on page 359 to add messages to the current Web communications comfort group.
11. Under **Group Messages**, use the arrow keys to configure the sequence of messages.
12. Click **Save**.

Changing the sequence of messages in a Web communications comfort group

Before you begin

- Set up a Web communications comfort group that is associated with Web communications skillset.

About this task

Follow this procedure to change the sequence in which comfort messages in a Web communications comfort group appear to customers.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.

3. Click **Comfort Messages**.
4. Under **Comfort Group**, select the comfort group to change.
5. Click **Edit**.
6. Under **Group Messages**, use the arrow keys to configure the sequence of messages.
7. Click **Save**.

Deleting a message from a Web communications comfort group

Before you begin

- Set up a Web communications comfort group that is associated with Web communications skillset.

About this task

Follow this procedure to delete a comfort message from a Web communications comfort group, if you do not want to use that message in a Web communications comfort group.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Comfort Messages**.
4. Under **Comfort Group**, select the **Group** that contains the **Message** to delete.
5. Click **Edit**.
6. Under **Group Messages**, select the **Message** to delete.
7. Under **Edit Group**, click **Remove**.

   The system displays a Warning dialog box.
8. Click **Yes** to confirm the decision.
9. Click **Save**.

Deleting a Web communications comfort group

Before you begin

- Set up a Web communications comfort group that is associated with Web communications skillset.

- Ensure that the Web communications comfort group is unlinked from any other skillset before it is removed.

About this task

Follow this procedure to delete a Web communications comfort group if you do not want to use that comfort group.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Comfort Messages**.
4. Under **Comfort Group**, select the **Group** to delete.
5. Click **Delete**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the deletion.

Configuring intrinsics for agent-supervisor observe and barge-in

About this task

An agent-supervisor can observe or barge-into any active incoming agent-customer Web Communications chat session of all agents under the supervision of the agent-supervisor. Agent Desktop displays active incoming Web Communications contacts and Voice contacts to agent-supervisors.

Agent Desktop flags any Web Communications contacts where certain intrinsic values exceed the defined threshold.

Using the Multimedia Administration utility, you can set the threshold values for intrinsics. Some of the intrinsics are:

- Conversation Length (seconds)
- Seconds since last message out
- Seconds since last message in
- Number of Agent Messages
- Unanswered Messages

Using the Multimedia Administration utility, you can assign a priority from 1 to 5, 1 being the highest priority, to each of the intrinsics. The system uses the threshold and priority values assigned to sequence the Web Communications contacts in a list. Contacts which require urgent attention appear at the top of this list.

Important:

Each intrinsic type has a unique priority level. For example, Conversation Length and Customer Idle Time intrinsics cannot have the same priority level.

If the value set for the intrinsics exceeds the defined threshold, the system flags the contact as requiring attention. If the system flags more than one contact, then these contacts are sequenced based on a weightage. The system calculates this weightage using the priority of the intrinsic with exceeded thresholds. A higher weightage is given to intrinsics that have a higher priority.

For example, if contact A has exceeded the threshold for intrinsics of priority 1 and 2, and contact B has exceeded the threshold for intrinsics of priority 1 and 3, then contact A appears above contact B in the list.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Web Comms**.
3. Click **Intrinsic Settings**.
4. Under **Intrinsic Data**, type a number of seconds or type a number in the **Threshold** box.
5. Under **Intrinsic Data**, select a number, from 1 to 5, in the **Priority** drop-down box.

   Each intrinsic type has to have a unique priority level.
6. Click **Save**.

Chapter 33: Agent Desktop configuration

The Contact Center Multimedia Administrator application includes settings that you use to configure properties for Agent Desktop. These settings allow agents to access database information and work with contacts.

Perform the procedures in this chapter to configure the Agent Desktop settings.

Note:

Some Agent Desktop settings on the Multimedia Administration tool require that you log on to CCMA from a Web browser on the CCMM server. These settings are:

- Agent Desktop Configuration
  - General Settings
  - Basic Screenpops
  - Advanced Screenpops
  - User Settings
  - Shortcut Keys

If your Contact Center uses Enterprise Web Chat (EWC), agents handling Web Communications contacts do not use Agent Desktop. These agents use a custom desktop that you develop using an SDK. The SDK documentation specifies the configuration file through which you configure settings for the custom desktop.

Adding a friendly name for a web chat agent

About this task

From Release 7.0 Feature Pack 1, Contact Center administrators can add a friendly name or nickname for a web chat agent.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **General Administration**.
3. Click **Agent Settings**.

4. In Edit Single Agent Settings, in the **Friendly name** field, type the friendly name for the web chat agent.

   The rules for the friendly name are similar to the rules for first name, which are as follows:

   - Can have a maximum of 30 characters
   - Can have white spaces
   - Cannot have the following characters: "!""#$%&*+/:;<=>?@[\]^`{|}~"

5. Click **Save**.

Next steps

Administrators must also choose the label that gets displayed in agents' responses to text chat messages with the contact. Administrators can also choose that the friendly name is displayed in welcome messages. For more information, see Configuring welcome messages and text chat labels on page 344.

Controlling access to email message text

About this task

Agents, by default, cannot edit text in an email message. You can either enable particular agents or enable all agents to delete text from email messages that enter the contact center.

For example, select this feature so agents can delete credit card information from an email message to protect confidential customer information.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **General Administration**.
3. Click **Agent Settings.**
4. Select the **Enable E-mail Text Deletion For All Agents** check box, to enable all agents to delete text from email messages.

   OR

   Click the agent, and under **Delete Enabled**, click the **Yes** option, to enable that agent to delete text from email messages.

5. Click **Save**.

Configuring supervisor approval for email messages on a per agent basis

About this task

Supervisors can approve email messages before the email messages reach the customers.

Note:

The approval process applies to email contacts only. The approval process does not apply to other contact types such as Fax, Scanned Documents, and SMS.

The approver of the email messages is the supervisor assigned to the approval skillset of the contacts that the agent handles.

Note:

Agents can pull contacts for approval. Restrict agents from pulling contacts for approval by configuring skillset partitions. For more information see, Configuring agent access to contacts on page 365.

You can configure the system to send email messages to supervisors for their approval on a per agent basis or per skillset basis. For more information, see Supervisor approval of email messages on page 210 and Configuring supervisor approval for email messages on a per skillset basis on page 271.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **General Administration**.
3. Click **Agent Settings**.
4. From the right pane, select an agent.
5. Under Edit Agent Settings in the **Email Approval Ratio** field, type the percentage of email messages that require supervisor approval for the agent.

   The approval ratio must be whole numbers ranging from 0 to 100.
6. Click **Save**.

Configuring agent access to contacts

About this task

Agents, by default, see all contacts in the contact center. You can restrict the access to show agents only the contacts assigned to the agent's skillsets. You can also apply these restrictions for multimedia contact transfers. Partitioning changes do not take effect until after an agent logs out and logs in again.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. Under **Agent Skillset Partitioning**, select **Enable Partitioning**.
5. If you want to apply partitioning rules when an agent transfers a multimedia contact, select **Apply Partitioning to Transfers**.
6. Click **Save**.

Disabling the Avaya Agent Desktop embedded softphone

About this task

Contact Center administrators can disable the Avaya Agent Desktop embedded softphone either on a per agent basis or on a system-wide basis. When the administrators disable the embedded softphone, Avaya one-X® Communicator can run concurrently with Avaya Agent Desktop.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **General Administration**.
3. Click **Agent Settings**.
4. To disable the Avaya Agent Desktop embedded softphone, perform one of the following:
   - To disable the softphone on a per agent basis, ensure that the **Enable integrated softphone** check box is cleared. By default, the **Enable integrated softphone** check box is selected.
   - To enable the softphone on a system-wide basis, click the **Enable integrated softphone for All Agents** check box.

     To disable the softphone on a system-wide basis, click the **Disable integrated softphone for All Agents** check box.

   CCMM Administration displays whether agents have the softphone enabled or disabled in the **Enable Softphone** column.
5. Click **Save**.

Creating or changing custom fields in Agent Desktop

About this task

You can add a custom field to the Agent Desktop for multimedia contacts that pertains to your contact center. For example, if your customers subscribe to a magazine, you can view information about each customer's subscription expiry date.

The value entered by the contact center agent for each customer appears in the custom field, the same as any other customer-entered information such as email address or phone numbers.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Resources**.
4. In the first blank row under **Current Custom Fields**, type the name of a custom field.

   OR

   Click on an existing field to change the label.
5. Press **Tab** to save your changes.

Deleting a custom field in Agent Desktop

About this task

Delete a custom field from the Agent Desktop when it is not required.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Resources**.
4. Under **Current Custom Fields**, select a custom field.

5. Press **Delete** on your keyboard.

   The system displays a Warning dialog box.

6. Click **Yes** to confirm the decision.

Configuring the active contact timer

About this task

Configure the maximum amount of time that you want a multimedia contact to remain open on a desktop. The active contact timer does not apply to Web communications contacts.

When this time expires, the contact remains open for a maximum of one more hour. Agent Desktop force closes the contact when the additional hour expires. Agent Desktop warns the user when the contact has 60 minutes, 30 minutes, and 5 minutes left before force closing the contact.

The default time in the Contact Center Multimedia configuration is one hour.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. In the **Maximum Open Duration** box, type the maximum amount of time you want multimedia contacts to remain active in hours and minutes.

   The minimum is 10 minutes and the maximum is 12 hours.

5. Click **Save**.

Configuring the callback timer

About this task

Configure the callback timer as a range of minutes to days for the system to wait before reoffering a pending contact to agents. An agent can delay the contact or place the contact into pending state because they are waiting for additional information to complete the contact.

The callback timer can be 2 minutes to 200 days (about 6 months). The default range provides the limits to which the you configure the callback time. The actual time value appears by default in the Agent Desktop application when the agent reschedules the contact.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. Under **Callback Time**, type a number of minutes in the **Minimum Time** box.
5. Under **Callback Time**, type a maximum number of days in the **Maximum Time** box.
6. Click **Save**.

Configuring the callback trunk access

About this task

Configure the callback trunk access to ensure that you can create a callback to the customer you work with. Callback trunk access enables you to schedule callbacks with customers who requested callbacks.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. Under **Callback Trunk Access**, type the trunk access number in the **Trunk Access Code** box.
5. Click **Save**.

Specifying the attachment size

About this task

Specify the maximum size of the attachments that an agent can attach to an email message.

Important:

The maximum file size set for attachments also applies to inline attachments.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. Under **Attachment Upload Size**, in the **Maximum Size** box, type the maximum number of kilobytes for a file.
5. Click **Save**.

Configuring Agent Desktop behavior

About this task

You can configure Agent Desktop to alert the agent when a new contact arrives. The alert can be one or more of the following methods:

- Bring Agent Desktop to the front.
- Give focus to Agent Desktop.

Important:

Changes you make to Agent Desktop configuration take effect only when agents restart Agent Desktop.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. Under **New Contact Presentation**, select the check boxes that describe the presentation.

Choose **Bring to front** or **Give focus**.

5. Click **Save**.

Variable definitions

Name	Description
New Contact Presentation	The method in which contacts are presented: • Bring to front: The Agent Desktop moves to the front upon arrival of a new contact. If Bring to front is disabled while Give focus is enabled, the Agent Desktop makes a warning sound and the toolbar flashes, but it is not brought to the front. • Give focus: The Agent Desktop window is the active window when it moves to the front. The Bring to Front check box must be selected for the Give Focus check box to be enabled.

Configuring the state of the Agent terminal on log off

About this task

Configure the agent terminal to be in idle or busy state when the agent logs off of the Agent Desktop. This setting is available only in AML-based contact centers.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. Under **Logoff Terminal State**, select **Idle** or **Busy**.
5. Click **Save**.

Configuring hotdesking

About this task

Configure your contact center so that an agent can sit at a different desk every day and log on to the Agent Desktop. With hotdesking enabled and properly configured, when agents start Agent Desktop, they automatically map to the relevant terminal and addresses without user intervention.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Agent Desktop Configuration**.
3. Select **General Settings**.
4. Under **Hot Desking**, select the **Enabled** check box.
5. Click **Save**.

Configuring hotdesking in a Citrix environment

About this task

When hotdesking is configured for a Citrix environment, agents see a dialog box that prompts them to enter a string that identifies their workstation. The string must be the same as the string that is configured as the workstation name in the Communication Control Toolkit configuration. You must configure the dialog box in a Citrix environment.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. Under **Hot Desking**, select the **Prompt for WorkStation** check box.
5. Click **Save**.

Configuring Web statistics

About this task

Configure Web statistics, so that agents and supervisors can use Agent Desktop to view real-time statistics for call handling, skillset data, and state information on Agent Desktop.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Agent Desktop Configuration**.
3. Select **General Settings**.

4. Under **Web Statistics**, select **Enabled**.
5. Click **Save**.

Configuring Web reporting

About this task

Enable Web reporting so that Contact Center reports on peer-to-peer Instant Messaging (IM). If an agent initiates an IM while active on a Contact Center contact, Contact Center reports on this activity.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Agent Desktop Configuration**.
3. Select **General Settings**.
4. Under **Web Reporting**, select **Enabled**.
5. Click **Save**.

Creating or changing a closed reason

About this task

Indicate a reason for closing a contact.

If one or more closed reasons are configured, then the agent must choose a closed reason to close the contact; otherwise, the agent need select no reason.

You can choose a default closed reason for each type of contact. See Configuring default closed reasons on page 374.

You can also assign a default closed reason to each contact type. The default reason is selected in the Agent Desktop application. The agent can choose another closed reason when closing a contact.

Important:

You cannot modify a default closed reason code.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Resources**.
4. Under **Closed Reason**, type a name for the **Closed Reason**.
5. Under the **Type** box, select **All** or the type of contact for each closed reason.
6. Press **Tab** to save your changes.

Configuring default closed reasons

Before you begin

- Create a closed reason. See Creating or changing a closed reason on page 373.

About this task

You can specify a default closed reason for each contact type (email, fax, SMS, Web communications, scanned document, and voice mail) in the contact center. A contact is automatically assigned the default closed reason code unless an agent changes it when the contact is closed.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Default Closed Reasons**.
4. In the **E-mail** drop-down box, select the configured closed reason to apply to email message contacts by default.
5. In the **Fax** drop-down box, select the configured closed reason to apply to email message contacts by default.
6. In the **SMS** drop-down box, select the configured closed reason to apply to SMS message contacts by default.
7. In the **Web Comms** drop-down box, select the configured closed reason to apply to Web communications contacts by default.

8. In the **Scanned Doc** drop-down box, select the configured closed reason to apply to scanned documents contacts by default.
9. In the **Voice Mail** drop-down box, select the configured closed reason to apply to voice mail contacts by default.
10. Click **Save**.

Deleting a closed reason

About this task

Delete a closed reason if you do not want the reason to appear in the Agent Desktop application. You cannot delete a default closed reason code.

Important:

You can delete only one row at a time.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Resources**.
4. Select a closed reason from the list.
5. Press **Delete** on your keyboard.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the decision.

Configuring Shortcut keys for Agent Desktop

About this task

You can configure shortcut keys that agents can use in Agent Desktop. Agents can use shortcut keys to perform common tasks in Agent Desktop more efficiently.

In the CCMM Administration utility, you can map shortcut keys to a list of activities that agents perform on Agent Desktop. The default keys are already specified in the CCMM Administration utility. However, you can choose to change the default keys as you see fit for operational reasons.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Shortcut Keys**.

   The system displays the list of shortcut keys, which are mapped to specific activities that agents perform on Agent Desktop.
4. Update the shortcut keys as required.

   Shortcut keys have the format of Ctrl + (Optional) additional modifier + an alphanumeric character.

   The (Optional) additional modifier is either Shift or Alt. The alphanumeric character is in the range [A-Z] or [0–9].

   For example, the shortcut key for Login / Logout is Ctrl + Shift + L.

   Note:

   If you select **NONE** in the additional modifier field and **NONE** in the alphanumeric field of a shortcut key for a task, then the shortcut key for that task is disabled. This means that agents cannot use the shortcut key to perform this task on Agent Desktop.

   For example, if we select **CTRL** + **NONE** + **NONE** for Login / Logout, then the shortcut key for Login / Logout is disabled. The agents cannot use shortcut keys to login to or logout from Agent Desktop.
5. Click **Save**.

   The system displays a Warning dialog box.
6. Click **Yes** to confirm the change.

Configuring Basic Screen Pops

About this task

Use the Basic Screenpop page to configure application shortcuts and intrinsics. Agent Desktop starts these applications either when Agent Desktop displays an alert for a work item or when an agent accepts a work item. You can choose which contact intrinsics Agent Desktop displays when an agent opens a contact.

By default, the screen pop intrinsics list includes the standard intrinsics that are present on any contact that Contact Center handles. You can add a new intrinsic to this list, and select the intrinsic. The new intrinsic must already exist as a variable in Orchestration Designer, and must be populated with a value so that the screen pop can use the intrinsic.

Agent Desktop can display only the intrinsics relevant to the contact type. For example, Agent Desktop can display a From Address for an email contact, but not for a voice contact.

Agent Desktop can display multiple intrinsics for a contact. However, you can select just one intrinsic that Agent Desktop sends as a screen pop parameter to the Basic screen pop applications. Agent Desktop sends the same intrinsic to all the configured applications, but you can configure a different screen pop parameter for each contact type. For example, the screen pop parameter for voice contacts can be AD_CLID, and for email contacts it can be FROMADDRESS.

Ensure you configure a screen pop parameter that is valid for the contact type. See the following table for the list of valid intrinsics for each contact type. If you create a new intrinsic, ensure it is valid for a contact type before using the new intrinsic as a screen pop parameter.

Table 2: Valid intrinsics for each contact type

Contact type	Valid intrinsics
Voice	AD_CDN, AD_CLID, AD_DNIS, CCAD_IVR, ProviderContactID , Skillset, SIP_RETURNED_DIGITS_LAST, SIP_RETURNED_DIGITS_2LAST
Email	CONTACTID, FROMADDRESS, Skillset, TOADDRESS
Fax	CONTACTID, FROMADDRESS, Skillset, TOADDRESS
Instant Message	AD_CDN, AD_CLID, ProviderContactID, Skillset, SIP_FROM_ADDRESS, SIP_TO_ADDRESS, SIP_INITIAL_TEXT, SIP_RETURNED_TEXT_1
Outbound	CONTACTID, Skillset
Open Queue	CONTACTID, Skillset
POM Outbound	CONTACTID, Skillset
Scanned Document	CONTACTID, FROMADDRESS, Skillset, TOADDRESS
SMS	CONTACTID, FROMADDRESS, Skillset, TOADDRESS
Social Networking	CONTACTID, FROMADDRESS, Skillset, TOADDRESS
Voice Mail	CONTACTID, FROMADDRESS, Skillset, TOADDRESS
Web Communication	CONTACTID, Skillset

Note:

In AML-based contact centers, Contact Center retrieves intrinsics for CDN calls only, whereas in SIP-enabled contact centers, Contact Center retrieves intrinsics for both CDN and personal calls. For personal calls, the SIP_FROM_ADDRESS intrinsic is not populated on Agent Desktop.

If you want to use data collected from an IVR application in a SIP-enabled contact center, always use the SIP_RETURNED_DIGITS_LAST and SIP_RETURNED_DIGITS_2LAST intrinsics. Contact Center cannot guarantee that the SIP_RETURNED_DIGITS_n intrinsic contains the final data that the caller entered on the IVR application.

The following intrinsics are not available by default: ProviderContactID, SIP_FROM_ADDRESS, SIP_TO_ADDRESS, SIP_INITIAL_TEXT, SIP_RETURNED_TEXT_1. If you require these intrinsics, you must add them using the Multimedia Administration utility.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Basic Screenpops**.
4. Click the **General settings** tab to configure settings that apply to all Basic screen pops.

   The settings under the Global Screenpop settings and the Basic Screenpop settings sections apply to both Basic and Advanced screen pops. However, you can override the Basic Screenpop settings when you configure Advanced screen pops. For more information, see Configuring Advanced Screen pops on page 382.

   a. Select the **Allow Agents select Screen Pop(s)** check box to allow agents to choose the screen pop applications the agents require while using Agent Desktop.

   b. Select the **Auto Expand AAAD on Work Item Answer** check box to expand the Agent Desktop application when an agent responds to a work item.

   c. Select the **Launch Screen Pop on Incoming Personal Calls** check box to open screen pops during personal calls.

   d. Select the **Launch Screen Pop on Outgoing Personal Calls** check box to open screen pops during personal outbound calls.

   e. Select the **Launch Screenpop on Consultation received** check box to automatically open screen pops on the consulted agent's desktop after a contact consult or transfer starts.

   f. Select the **Launch Screenpop on Consultation initiating** check box to automatically open screen pops on the Agent Desktop of the agent who initiates the consult. The screen pop appears when the consult is initiated.

   g. Select the **Close Screenpop when Consult/Transfer is Completed** check box to automatically close screen pops after a contact consult or transfer is complete.

   h. Select the **Display Screenpops when Observe** check box to push the screen pop application from the original call to a supervisor/agent who is observing that call.

   i. Select the **Launch Screen Pop in a tab inside AAAD** check box to open the screen pop application within the Agent Desktop user interface.

      Only Web-based applications can open within Agent Desktop.

   j. Select the **Auto Close Screen Pop tab(s) on Work Item Release** check box to automatically close the screen pop tab on the Agent Desktop when an agent releases a contact.

   k. From the **Launch State** drop-down list, select the event type that opens Basic screen pops.

      Select Active for the screen pop applications to open when an agent answers a contact. Select Alerting for the screen pop applications to open when Agent Desktop

displays an alert for a contact. When a supervisor/agent observes a contact, Alerting works only for voice contacts, it does not work for any other contact type.

5. Click the **General Intrinsics** tab to set up the intrinsics that Agent Desktop can display and the intrinsics that Agent Desktop can pass as parameters to the screen pop applications.
   a. Under **Screen Pop Intrinsics**, configure the intrinsics used to display data to the agent.

      You can configure only one intrinsic as a screen pop parameter.

      For consults or transfers, Avaya Aura® Contact Center provides the Skillset intrinsic only on Email and Web Communications contacts, and not on Instant Messaging or Voice contacts.

   b. Click **Add** to add a new intrinsic.

      The name of the intrinsic you add must match the corresponding variable name in Orchestration Designer. The names are case-sensitive.

   c. Click **Contact Screen Pop Intrinsics** to set different screen pop parameter intrinsics for the configured contact types.

      You can select only one intrinsic for each contact type.

   d. Click **Personal Call Screen Pop Intrinsics** to set screen pop parameter intrinsics for applications that open on **Inbound** and **Outbound** personal calls.
6. Click the **Basic Screenpop Shortcuts** tab to configure applications for Basic screen pops.

   Use the **Basic Screenpop Shortcuts** tab to configure Basic screen pops. Basic screen pops consist of four parts:

   - **Name**: The **Name** field contains the name of the screen pop.
   - **Path**: The **Path** field contains the command that Agent Desktop uses to open the screen pop.
   - **Always on screenpop** check box: The **Always on screenpop** check box selects the applications that Agent Desktop opens as screen pops. Agent Desktop can open only five screen pop applications.
   - **Event**: The **Event** field shows the launch state that you set in the **General settings** tab. You cannot edit the **Event** field.

   a. Click **Add** to add a new screen pop application.

      You can configure a maximum of 20 Basic screen pops. However, you can select only five screen pops to open on Agent Desktop when a contact alerts or opens.

   b. Use the **Always on screenpop** check box to select the applications that Agent Desktop opens as screen pops when a contact alerts or opens.

      Text applications such as Notepad, or search engines such as Google can open automatically. You can add other applications, but you must ensure that the applications are installed on all clients.

7. Click the **Basic Filters** tab to select for which contact types Agent Desktop displays screen pops.

   Under the **Filter screenpops by Contact Types** list, select the contact types. Agent Desktop opens all Basic screen pops with **Always on screenpop** selected when one of the contact types you select alerts or opens.

   In a voice-only Contact Center, the **Basic Filters** tab shows only the **Voice** contact type.

8. Click **Save**.

Configuring Advanced screen pop applications

About this task

When configuring an Advanced screen pop, you must select an application that you want Agent Desktop to open. This procedure outlines the steps for configuring an Advanced application.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Advanced Screenpops**.

   The system displays the Advanced Screenpop Settings page.

4. Click the **Advanced Applications** tab.

   The system displays the Applications grid that contains the existing applications.

5. Click **New** to create a new application.

   The system displays the Create/Edit Application section at the bottom of the page.

6. Type the name of the application in the **Name** field.
7. Type the location of the application in the **Path** field.

   The path information can contain parameters.

   Note:

   You can assign a maximum of five parameters to each application.

8. To prevent mistakes when you type a parameter, click the **Insert Parameter** button to insert a parameter within a path.
9. Click **Save**.

   The system displays the new application under the Applications grid.

Configuring Advanced screen pop filters

About this task

When you are configuring Advanced screen pops, you can optionally select a filter for that Advanced screen pop. A filter defines additional conditions that must be met before an Advanced screen pop opens. These conditions match the contact intrinsic values with the predefined values. This procedure outlines the steps for configuring an Advanced filter.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Advanced Screenpops**.

   The system displays the Advanced Screenpop Settings page.
4. Click the **Advanced Filters** tab.

   The system displays the Filters grid that contains the existing filters.
5. Click **New** to create a new filter.

   The system displays the Create/Edit Filter section at the bottom of the page.
6. Type the name of the filter in the **Name** field.
7. From the **Intrinsic Type** field, select an intrinsic whose value is compared against a set of applicable values.

   Note:

   The method of defining these applicable values depends on the intrinsic type you select. If you select an intrinsic of type Skillset, CDN, or DNIS, you must select the applicable values from a list. Otherwise, you must type an instrinsic value to match against the applicable values in a text box under the Intrinsic Values section and click **Add >**.

   Agent Desktop opens screen pops based on the intrinsic type.
8. From the **Contact Types** list , select the contact types to which the filter is applicable.

   Note:

   If you select the intrinsic type as Skillset, the list of applicable values to compare against changes according to the contact types selected or deselected.
9. If you select an intrinsic of type Skillset, CDN, or DNIS, select the applicable values from the list of values the system displays under the Intrinsic Values section.

   Or

   Type an instrinsic value to match against the applicable values in a text box under the Intrinsic Values section and click **Add >**.

Contact Center Manager Server (CCMS) retrieves the intrinsic values if the intrinsic types are Skillset, CDN, and DNIS. You must correctly configure the intrinsic values in CCMS for this functionality to work.

Note:

If you add an intrinsic, the intrinsic must already exist as a variable in Orchestration Designer and must be populated so that the screenpop can use the intrinsic.

10. Click **Save**.

    The system displays the new filter under the Filters grid.

Configuring Advanced Screen pops

About this task

Use Advanced Screen pops to configure individual screen pops to open on specific intrinsic triggers and filters. Advanced Screen pops provide administrators with greater range and flexibility with respect to conditions and triggers for opening a particular screen pop. However, administrators must configure the screen pop application to open based on one intrinsic. For example, configure a Web page (application) to open when you receive a contact with skillset EM_Ramdom_Skillset (intrinsic).

A maximum of five screen pops can launch on Agent Desktop for each event. The order of opening the screen pops is as follows:

1. All Basic Screen pops that match the configured contact type, event, and intrinsic.
2. Advanced Screen pops that match the configured contact type, event, and filter. Advanced Screen pops open in an ascending order based on the screen pops configured on the Advanced Screenpop Settings page.

Note:

The Advanced Screenpops wizard displays the Screenpop Summary section at the bottom of each screen. Screenpop Summary summarizes the actions that a user performs to configure a screen pop. You can use Screenpop Summary as a reference when you are configuring screen pops.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **Advanced Screenpops**.

   The system displays the Advanced Screenpop Settings page.
4. Click the **Advanced Screenpops** tab.

The system displays the Advanced Screenpops grid that contains the existing screen pops. Select a screen pop and then click the up arrow (**^**) button or the down arrow (**v**) button to change the order of the screen pops. This affects the order in which the screen pops are evaluated for launch.

5. Click **New** to create a new screen pop.

   The system displays Step 1 of 7 — Name page of the New Screenpop wizard.

6. Type the name of the screen pop in the **Screenpop Name** field.

   Screen pop names must be unique.

7. Click **Next**.

   The system displays Step 2 of 7 — Contact Types page of the New Screenpop wizard.

8. From the **Contact Types** list, select the contact types. The screen pop opens based on the selected contact types.

9. Click **Next**.

   The system displays Step 3 of 7 — Launch Event page of the New Screenpop wizard.

10. From the **Launch Event** drop-down list, select the event to open the screen pop. You can select one of the following:

    - **Active**: The screen pop application opens when an agent answers a contact.
    - **Alerting**: The screen pop application opens when Agent Desktop displays an alert for a work item.

    Note:

    A maximum of five screen pops can launch on Agent Desktop for each event.

11. Click **Next**.

    The system displays Step 4 of 7 — Application page of the New Screenpop wizard.

12. From the **Application Name** drop-down list, select the application that opens on client computers when Agent Desktop displays the screen pop.

    Or

    Click the Add (**+**) icon to add a new screen pop application. For more information, see Configuring Advanced screen pop applications on page 380.

    Or

    Select an existing application from the drop-down list and click **Edit** to edit an existing screen pop application.

    Note:

    Editing an existing application is supported only when the application is not in use.

Text applications such as Notepad, or search engines such as Google can start automatically. You can add other applications, but you must ensure that the applications are installed on all clients.

13. Click **Next**.

    The system displays Step 5 of 7 — Customise Application page of the New Screenpop wizard.

14. From the **Parameter** drop-down list, select a parameter that is present in the path.

    The number of parameters depends on the number of placeholders configured in the application on page Step 4 of 7 — Application.

    Note:

    You can set up to a maximum of five parameters for each screen pop application.

15. From the **Intrinsic** drop-down list, select an intrinsic value that replaces the parameter placeholder at runtime.

16. Click **Set**.

    The system displays the parameter and the corresponding intrinsic value under the Parameters section.

    Note:

    You must assign intrinsic values for all parameters present in the path.

17. Click **Next**.

    The system displays Step 6 of 7 — Filter page of the New Screenpop wizard.

18. **(Optional)** From the **Filter** drop-down list, select the filter for the screen pop.

    Or

    Click the Add (**+**) to add a new filter. For more information, see Configuring Advanced screen pop filters on page 381.

    Click **Edit** to edit an existing filter.

    Note:

    If you select a filter, Agent Desktop displays the screen pop only if matched conditions between the filter and the created screen pop are met.

    Only the filters containing all the contact types that you select from the **Contact Types** list on page Step 2 of 7 — Contact Types are available.

    If you select an existing filter, the system displays the filter conditions under the Selected Filter Conditions section. The Selected Filter Conditions section displays the intrinsic name and the corresponding values under the Match Values section.

19. Click **Next**.

The system displays Step 7 of 7 — Presentation Options page of the New Screenpop wizard.

The presentation options are set to the global settings that you have configured for Basic screen pops. However, for Advanced screen pops you can change these settings for each screen pop. For more information about global settings, see Configuring Basic Screen Pops on page 376.

20. Select the **Launch Screen Pop in a tab inside AAAD** check box to open the screen pop application within Agent Desktop.

    Only Web-based applications can open within Agent Desktop.

21. Select the **Auto Close Screen Pop tab(s) on Work Item Release** check box to automatically close the screen pop tab on Agent Desktop once an agent releases a contact.

22. Click **Finish**.

    The system displays the Saved dialog box.

23. Click **OK**.

    The system displays the new screen pop under the Advanced Screenpops grid.

Enabling Customer History on Voice Contacts

Before you begin

- Use the administration tool on a Contact Center Multimedia server in order to configure customer history on voice contacts.
- Enable Contact Summary Data generation in Contact Center Manager Administration, to ensure that individual contact history data is created in the Contact Center Manager Server database.

About this task

You can search for customer history based on the calling line ID for voice contacts.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **Agent Desktop Configuration**.
3. Click **User Settings**.
4. Select **True** in the **Display Customer History on Voice Contact** list, to display customer history for voice contacts in Agent Desktop.

5. In the **Voice Contact Identifier for Customer History** list, select the parameter to lookup the CCMM database that contains customer history for the originator of the incoming voice call.
6. Select **True** in the **Display Voice Calls in Customer History** list to display previous voice calls for the originator of the current active contact in Agent Desktop. Enable this setting to lookup the Contact Center Manager Server database for Voice Contact history.

   Important:

   Ensure that you have entered the port number that is used by the Agent Desktop to connect to the Contact Center Manager Server in the Voice History Port box in the Multimedia, Agent Desktop Configuration, and Advanced Settings page for retrieving the voice history information.
7. Click **Save**.

Restricting file extensions for attachments

About this task

You can use the CCMM Administration utility to configure the supported list of file extensions that agents can attach to emails.

Note:

This procedure does not apply to voice-only contact centers. To enable this multimedia feature, obtain and configure a multimedia-enabled license.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, click **General Administration**.
3. Click **Agent Settings**.
4. Click **User Settings**.
5. To configure file extensions, perform one of the following:
   a. To add a new extension, type the file extension in the **Supported attachment file extensions** field and click **Add**.

      You must add the file extension in the description with the appropriate file extensions format. Each file extension must be separated by a semicolon (;).

      For example, if you want to add Word documents as a supported file extension, type `Word documents (*.doc;*.docx)`.
   b. To remove a file extension, select the file extension from the **Current supported file extensions** field and click **Remove**.

6. Click **Save**.

Configuring Advanced Settings

About this task

You can specify advanced configuration settings for Agent Desktop.

Note:

This procedure does not apply to voice-only contact centers. For voice-only contact centers, see Configuring Advanced Settings in a voice-only solution on page 391.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Agent Desktop Configuration**.
3. Click **General Settings**.
4. On the General Settings screen, click **Advanced**.
5. Update the required settings.
6. Click **Save**.

Variable definitions

Name	Description
Platform	The type of platform that your contact center uses. Select one of the following: • SIP. Select this option for a SIP-based contact center. • AML. Select this option for an Avaya Communication Server 1000-based contact center.
Switch Type	The type of PABX that you use in your contact center for voice contacts. When you select **SIP** as the platform type, following are the possible values for the Switch Type: • Sip Avaya Aura 6.2FP4 / 7.0. Select this option when integrating Avaya Aura® Contact Center

Table continues…

Name	Description
	with an Avaya Aura® Unified Communications platform Release 6.2 FP 4 or later. • CS1K • IP Office When you select **AML** as the platform type, the Switch Type must be CS1K.
IM Provider (SIP Contact Center only)	Select your Instant Messaging (IM) provider type to enable Presence on Agent Desktop and peer-to-peer Instant Messaging between agents and experts. Select one of the following: • None • Lync 2010 / Lync 2013 **Note:** Select this option also for Microsoft Skype for Business. • Aura Presence Services **Note:** You can select **Aura Presence Services** only if you select **Sip Avaya Aura 6.2FP4 / 7.0** in the **Switch Type** list.
IM Consult Reporting on Voice Contacts (SIP Contact Center only)	Enable or disable the reporting of IM or Multimedia consults by agents on voice contacts.
Agent Web Statistics	Enable Agent Web Statistics on Agent Desktop, so that agents and supervisors can use Agent Desktop to view statistics for call handling, skillset data, and state information on Agent Desktop.
Voice History Port	Enter the port number on CCMS that Agent Desktop connects to for retrieving the voice history information. Voice history information contains details of previous voice calls to the Contact Center from the dialed number of the currently active contact. **Note:** The default port is 443 with the security feature on which is the default value. In case you have disabled the security feature, the default port is 80. You cannot change the value of the port.

Table continues…

Name	Description
Number of Simultaneous Web Comms Observe/ Barge-in Contacts	Enter the maximum number of Web Communications contacts that a supervisor can observe or barge-in on simultaneously.
Web Comms Observe/Barge-in Refresh Rate	Enter the time, in seconds, at which the multimedia intrinsics and chat summary refreshes for each Web Communications contact in the **Supervisor Observe: Contact** list on Agent Desktop.
Number of Messages to Display in Web Comms Observe/Barge-in Summary	Enter the number of messages to display in the chat summary for the selected Web Communications contact in the **Supervisor Observe: Contact** list on Agent Desktop. Agent Desktop displays the newest messages first in the list. For example, if this value is 5 and a supervisor selects a Web Communications contact containing 6 messages, then the summary displays messages from 2 to 6.
Contact Center LDAP Phone Book	Enable the Contact Center LDAP Phonebook to provide agents with a list of other agents, whom they can consult, during a voice call or an email contact.
Contact Types That Can Be Observed	Select the contact types that agent supervisors can observe. You can select either **Voice** or **Web Communications** or both.
IM Logging	Select the **IM Logging** check box to capture IM/ Presence server log messages in Agent Desktop log files.
Web Stats Logging	Select the **Web Stats Logging** check box so that Agent Desktop log files capture log messages relating to the Web Statistics feature. **Note:** **Web Stats Logging** generates logging inside Agent Desktop only.
Web Comms Logging	Select the **Web Comms Logging** check box so that Agent Desktop log files capture log messages for the Web Communications server. **Note:** **Web Comms Logging** generates logging inside Agent Desktop only.
CCT Logging Level	Select the logging level that Agent Desktop log files capture for CCT. You can choose from the following: • **Off**

Table continues…

Name	Description
	• **Verbose** **Note:** **CCT Logging Level** generates logging inside Agent Desktop only.
Enable Reason Code Logging	Select the **Enable Reason Code Logging** check box so that Agent Desktop log files capture log messages for reason codes that agents enter during a contact. **Note:** **Enable Reason Code Logging** generates logging inside Agent Desktop only.
Enable Advanced Audio Controls for Softphone	Select the **Enable Advanced Audio Controls for Softphone** check box to allow an agent to control Receive Gain and Transmit Gain, which allows agents to change the audio level of the incoming and outgoing speech path when Agent Desktop is in the My Computer mode.
LDAP Phonebook Unique Key	Enter the LDAP attribute that Agent Desktop uses to uniquely identify any entries that agents search for in the LDAP server. The default value is objectGUID, which is the default Microsoft Active Directory unique identifier.
LDAP Phonebook Display Name	Enter the LDAP attribute that Agent Desktop uses as the primary display field in Phonebook.
Barge-in Wait Time	Enter the time in seconds between a Supervisor initiating an observe and having the ability to initiate a barge-in on the same contact. The default value is 5 seconds.
Supervisor Observe window refresh delay	Enter the time in seconds between an agent answering a new contact and the supervisor control refreshing to display this contact. The default value is 1 second.
Replace + with trunk access code	Select the **Replace + with trunk access code** check box so that Agent Desktop Phonebook adds a trunk access code before dialing any number. Therefore, agents do not need to manually add a leading digit to call externally or forward a call using Phonebook. By default, **Replace + with trunk access code** is selected.

Table continues…

Name	Description
Auto Sign On to CCMM	Select the **Auto Sign On to CCMM** check box so that agents do not need to login separately to CCMM when logging on to Agent Desktop.

Configuring Advanced Settings in a voice-only solution

About this task

You can specify advanced configuration settings for Agent Desktop in a voice-only solution.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Agent Desktop Configuration**.
3. Click **General Settings**.
4. On the General Settings screen, click **Advanced**.
5. Update the required settings.
6. Click **Save**.

Variable definitions

Name	Description
Platform	The type of platform that your contact center uses. Select one of the following: • SIP. Select this option for a SIP-based contact center. • AML. Select this option for an Avaya Communication Server 1000-based contact center.
Switch Type	The type of PABX that you use in your contact center for voice contacts. When you select **SIP** as the platform type, following are the possible values for the Switch Type: • Sip Avaya Aura 6.2FP4 / 7.0. Select this option when integrating Avaya Aura® Contact Center

Table continues…

Name	Description
	with an Avaya Aura® Unified Communications platform Release 6.2 FP 4 or later. • CS1K • IP Office When you select **AML** as the platform type, the Switch Type must be CS1K.
IM Provider (SIP Contact Center only)	Select your Instant Messaging (IM) provider type to enable Presence on Agent Desktop and peer-to-peer Instant Messaging between agents and experts. Select one of the following: • None • Lync 2010 / Lync 2013 **Note:** Select this option also for Microsoft Skype for Business. • Aura Presence Services **Note:** You can select **Aura Presence Services** only if you select **Sip Avaya Aura 6.2FP4 / 7.0** in the **Switch Type** list.
IM Consult Reporting on Voice Contacts (SIP Contact Center only)	Enable or disable the reporting of IM or Multimedia consults by agents on voice contacts.
Agent Web Statistics	Enable Agent Web Statistics on Agent Desktop, so that agents and supervisors can use Agent Desktop to view statistics for call handling, skillset data, and state information on Agent Desktop.
Voice History Port	Enter the port number on CCMS that Agent Desktop connects to for retrieving the voice history information. Voice history information contains details of previous voice calls to the Contact Center from the dialed number of the currently active contact. **Note:** The default port is 443 with the security feature on which is the default value. In case you have disabled the security feature, the default port is 80. You cannot change the value of the port.

Table continues…

Name	Description
Contact Center LDAP Phone Book	Enable the Contact Center LDAP Phonebook to provide agents with a list of other agents, whom they can consult during a voice call.
Contact Types That Can Be Observed	Select the contact types that agent supervisors can observe. You can select either **Voice** or **Web Communications** or both. **Note:** For voice-only contact centers, you can select only **Voice**.
IM Logging	Select the **IM Logging** check box to capture IM/ Presence server log messages in Agent Desktop log files.
Web Stats Logging	Select the **Web Stats Logging** check box so that Agent Desktop log files capture log messages relating to the Web Statistics feature. **Note:** **Web Stats Logging** generates logging inside Agent Desktop only.
CCT Logging Level	Select the logging level that Agent Desktop log files capture for CCT. You can choose from the following: • **Off** • **Verbose** **Note:** **CCT Logging Level** generates logging inside Agent Desktop only.
Enable Reason Code Logging	Select the **Enable Reason Code Logging** check box so that Agent Desktop log files capture log messages for reason codes that agents enter during a contact. **Note:** **Enable Reason Code Logging** generates logging inside Agent Desktop only.
Enable Advanced Audio Controls for Softphone	Select the **Enable Advanced Audio Controls for Softphone** check box to allow an agent to control Receive Gain and Transmit Gain, which allows agents to change the audio level of the incoming and outgoing speech path when Agent Desktop is in the My Computer mode.
LDAP Phonebook Unique Key	Enter the LDAP attribute that Agent Desktop uses to uniquely identify any entries that agents search

Table continues…

Name	Description
	for in the LDAP server. The default value is objectGUID, which is the default Microsoft Active Directory unique identifier.
LDAP Phonebook Display Name	Enter the LDAP attribute that Agent Desktop uses as the primary display field in Phonebook.
Barge-in Wait Time	Enter the time in seconds between a Supervisor initiating an observe and having the ability to initiate a barge-in on the same contact. The default value is 5 seconds.
Supervisor Observe window refresh delay	Enter the time in seconds between an agent answering a new contact and the supervisor control refreshing to display this contact. The default value is 1 second.
Replace + with trunk access code	Select the **Replace + with trunk access code** check box so that Agent Desktop Phonebook adds a trunk access code before dialing any number. Therefore, agents do not need to manually add a leading digit to call externally or forward a call using Phonebook. By default, **Replace + with trunk access code** is selected.
Auto Sign On to CCMM	Select the **Auto Sign On to CCMM** check box so that agents do not need to login separately to CCMM when logging on to Agent Desktop.

Configuring User Settings

About this task

The User Settings page contains configuration settings that you can customize for the Agent Desktop.

Note:

This procedure does not apply to voice-only contact centers. For voice-only contact centers, see Configuring User Settings in a voice-only solution on page 408 for User settings.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Agent Desktop Configuration**.
3. Click **User Settings**.
4. Update the required settings.

5. Click **Save**.

Variable definitions

Name	Description
Open Queue Contact Processing	Select the **Open Queue Contact Processing** check box to use Contact Center Multimedia to route multimedia contacts to agents by using the existing scripting and skillset routing features available for calls. You must install and license the Open Queue feature for Agent Desktop and configure Open Queue on the Communication Control Toolkit server.
Display Customer History on Voice Contact	Select the **Display Customer History on Voice Contact** check box to display customer history for voice contacts on Agent Desktop. Contact Center Multimedia searches for customer history of previous contacts based on the calling line ID for voice contacts.
Display Customer History on Personal Calls (SIP-enabled Contact Center only)	Select the **Display Customer History on Personal Calls** check box to display customer history for voice contacts on personal calls on Agent Desktop.
Voice Contact Identifier for Customer History (SIP-enabled Contact Center only)	Select either **AD_CLID** or **SIP_FROM_ADDRESS** to look up the Contact Center Multimedia database that contains customer history for the originator of the incoming voice call. In order to search the database you must also enable the Voice Contact Search parameter.
Encoding Page of CCT Attached Data	Enter the value that determines the decode Code Page used to convert the Binary Attached Data stream to a String contact types for the configured intrinsics. This is used to retrieve the Skillset Name in an AML Contact Center. The system supports the following cases: • The default encoding, that is, the encoding specified in the regional settings for the computer executing this method • little-endian Unicode (UTF-16LE) • big-endian Unicode (UTF-16BE) • Windows operating system (windows-1252) • UTF-7 • UTF-8

Table continues…

Name	Description
	• ASCII • Latin1 • GB18030 (Chinese Simplified) • CodePage Name • 1200 “UTF-16LE”, “utf-16”, “ucs-2”, “unicode”, or “ISO-10646-UCS-2” • 1201 “UTF-16BE” or “unicodeFFFE” • 1252 “windows-1252” • 65000 “utf-7”, “csUnicode11UTF7”, “unicode-1-1-utf-7”, “unicode-2-0-utf-7”, “x-unicode-1-1-utf-7”, or “x-unicode-2-0-utf-7” • 65001 “utf-8”, “unicode-1-1-utf-8”, “unicode-2-0-utf-8”, “x-unicode-1-1-utf-8”, or “x-unicode-2-0-utf-8” • 20127 “us-ascii”, “us”, “ascii”, “ANSI_X3.4-1968”, “ANSI_X3.4-1986”, “cp367”, “csASCII”, “IBM367”, “iso-ir-6”, “ISO646-US”, or “ISO_646.irv:1991” • 54936 “GB18030”
Attachment Upload Timeout	Enter the time in seconds after which the Communication Control Toolkit server session expires during uploading an attachment.
Suppress Browser Script Errors	Select the **Suppress Browser Script Errors** check box to suppress browser script errors.
Display Not Ready Reason Text Only	Select the **Display Not Ready Reason Text Only** check box to display only not ready reason text.
Display Voice Calls in Customer History	Select the **Display Voice Calls in Customer History** check box to display previous voice calls for the originator of the current active contact in Agent Desktop. Enable this setting to lookup the Contact Center Manager Server database for Voice Contact history. Enable **Contact Summary Data generation** in Contact Center Manager Administration, to ensure that individual contact history data is created in the Contact Center Manager Server database.
Number of Personal IM's Allowed To Go Ready	Enter the maximum number of open IM's an individual agent is allowed before the agent is not allowed to go ready. The number of personal IM's an agent is allowed open on Agent Desktop at one time cannot exceed the number configured in this field.

Table continues…

Name	Description
Audible Alert Setting	Select the type of alert Agent Desktop plays when contacts are presented to agents. There are four options: • NONE. No alert is played. • BEEP. The agents internal sound card is played as the alert. • WAV. A .wav audio file is played as the alert. • BOTH. Both the WAV and BEEP settings work.
Play Alert on Voice	Select the **Play Alert on Voice** check box to ensure an alert is played when voice contacts are presented to agents.
Play Alert on CCMM	Select the **Play Alert on CCMM** check box to ensure an alert is played when multimedia contacts are presented to agents.
Source of WAV	Select MM or SPARK. This determines whether the .wav file played is a CCMM .wav file or the .wav file from the Agent Desktop Spark Emulator.
Display Caller's Friendly Name	In a SIP-enabled contact center, select the **Display Caller's Friendly Name** check box to enable a friendly name display on Agent Desktop for DN calls. When this is enabled, when one contact center agent receives a call from another contact center agent, the name of the calling agent (as configured in CCMA) displays on the Agent Desktop of the called agent. If a contact center agent receives a CDN call from another contact center agent, the friendly name displayed on the Agent Desktop of the called agent is the name of the calling agent as configured on Avaya Aura® Communication Manager. **Note:** Both agents must be configured in CCMA for the friendly name to be displayed on Agent Desktop.
Highlight DN Call During Transfer	Determines which leg of the call has focus in Agent Desktop during a supervised transfer scenario, the original customer leg or the DN leg to the transfer party. Select the **Highlight DN Call During Transfer** check box to focus the DN leg to the transfer party in Agent Desktop during a supervised transfer scenario.

Table continues…

Name	Description
Put Call on Hold During Transfer for the Phonebook	Select the **Put Call on Hold During Transfer for the Phonebook** check box to place the customer call on hold when an agent initiates a call transfer, using the Phonebook on Agent Desktop.
Observe Agent Initiated Contact Center Calls (SIP-enabled Contact Center only)	Select the **Observe Agent Initiated Contact Center Calls** check box to allow agent-supervisors to use the Observe function to listen in on an agent-initiated voice contact.
Taskbar Alert on New WebComms Message	Select the **Taskbar Alert on New WebComms Message** check box to configure a taskbar alert, when a new web communication message arrives on Agent Desktop.
Avaya Aura Presence Delay Factor (Miliseconds)	Enter the delay, in milliseconds, between releasing an IM connection and the corresponding CCT contact. This is required if the IM wrapup message is not being delivered to customers.
Clear Previous Phone Number	Select the **Clear Previous Phone Number** check box to clear the number of the previous voice contact present on Agent Desktop.
Clear Previous E-mail Address	Select the **Clear Previous E-mail Address** check box to clear the email address of the previous email contact present on Agent Desktop.
Maximum Number of Agent Initiated E-mails	Enter the maximum number of email messages that an agent can initiate. **Note:** By default, the maximum number of email messages that an agent can initiate is 5.
Web Comms/IM Tab Blink Duration	Enter the time, in seconds, for which Web Communications or IM Tab must blink on Agent Desktop. **Note:** By default, the Web Communications tab or the IM tab blinks for 5 seconds on Agent Desktop.
Web Stats Ticker Duration	Enter the time, in seconds, for which the Web Statistics ticker displays for each skillset. **Note:** By default, the Web Statistics ticker displays for 10 seconds for each skillset on Agent Desktop.

Table continues…

Name	Description
Display Agent Login Duration	Select the **Display Agent Login Duration** check box to display the time that the agent is logged into Agent Desktop.
Show CCMM Contact ID in Workitem	Select the **Show CCMM Contact ID in Workitem** check box to display the Contact ID for multimedia contacts for the Work Item present on Agent Desktop.
Close IM Popout Window Automatically When Session Has Ended	Select the **Close IM Popout Window Automatically When Session Has Ended** check box to close the IM popout window automatically when the agent completes the IM contact on Agent Desktop. **Note:** **Close IM Popout Window Automatically When Session Has Ended** is applicable only to contact centers that have IM enabled and by default this check box is selected in the CCMM Administration utility.
Decline Personal IM Automatically When Agent Busy On Contact	Select the **Decline Personal IM Automatically When Agent Busy On Contact** check box to refuse personal IM messages automatically when the agent is busy with a contact on Agent Desktop. **Note:** **Decline Personal IM Automatically When Agent Busy On Contact** is applicable only to contact centers that have IM enabled and by default this check box is selected in the CCMM Administration utility.
Maximum Number of E-mail Recipients	Enter the maximum number of people to whom an agent can send an email message. **Note:** By default, the maximum number of people to whom an agent can send an email message is 30.
Force Send Emails	Select the **Force Send Emails** check box to provide agents with the option to override an email address validation failure and send an email message even when the system detects an invalid email address.
Mandatory Comments for Email Approval	Select the **Mandatory Comments for Email Approval** check box to make review comments

Table continues…

Name	Description
	mandatory when supervisors approve or reject an email message.
Pull Contact On Same Skillset Only	Select the **Pull Contact On Same Skillset Only** check box so that agents can pull contacts only from the skillsets that the agents are currently assigned to.
Show All Email Skillsets	Select the **Show All Email Skillsets** check box so that agents can see all the skillsets configured in Contact Center when they are initiating an outgoing email. If you do not select the **Show All Email Skillsets** check box, agents see only the email skillsets to which they are currently assigned.
Web Stats Refresh Interval	Enter the time in seconds after which the Web Statistics information refreshes. **Note:** By default, the Web Statistics information refreshes every 60 seconds. The minimum Web Stats Refresh Interval is 30 seconds.
Web Stats Exception Limit	Enter the number of Contact Center Web Statistics (CCWS) connection exceptions allowed before the system disables the statistics feature. **Note:** If you enter zero in the **Web Stats Exception Limit** field, the statistics feature is never disabled.
Number of Rings on Voice Alert	Enter the number of times the agent phone rings when a voice contact alerts on Agent Desktop. **Note:** By default, the agent phone rings 5 times when a voice contact alerts on Agent Desktop.
Number of Alert Tones for Multimedia Contacts	Enter the number of alert tones that can be defined for Multimedia contacts. **Note:** By default, 5 alert tones can be defined for Multimedia contacts.
Maximum Roster Size	Enter the maximum number of IM contacts that agents can add to the **My Contacts** list in Agent Desktop.

Table continues…

Name	Description
	Note: You can set a maximum of 150 contacts in the **Maximum Roster Size** field if Agent Desktop connects to Avaya Aura® Presence Services.
Force Logout Delay	Enter the time, in seconds, the system displays the `You've Been Logged Out` alert before shutting down Agent Desktop, after a supervisor remotely logs an agent out of Contact Center from the Contact Center Manager Administration (CCMA) user interface. **Note:** By default, the system displays the `You've Been Logged Out` alert for 60 seconds.
Display System Defined Contact Center Codes	Select the **Display System Defined Contact Center Codes** check box so that Agent Desktop displays system-defined Not Ready Reason Codes and After Call Work Item codes.
Contact Center Code Display Preference	Select how Agent Desktop displays Contact Center codes. You can choose from the following: • Code. Agent Desktop displays Contact Center codes based on the code number. • Text. Agent Desktop displays Contact Center codes based on the code text. • Both. Agent Desktop displays Contact Center codes based on both the code number and the code text. **Note:** You can select **Contact Center Code Display Preference** only if you select the **Display System Defined Contact Center Codes** check box.
Enable Keyboard Shortcuts	Select the **Enable Keyboard Shortcuts** check box so that shortcut keys are enabled in Agent Desktop, and agents can use shortcut keys to perform common tasks on Agent Desktop. **Note:** By default, **Enable Keyboard Shortcuts** is selected in the CCMM Administration utility.

Table continues…

Name	Description
Allow Custom Contacts	Select the **Allow Custom Contacts** check box so that agents can add custom contacts to Phonebook in Agent Desktop. Custom contacts are personal contacts of the agents and are not present in the LDAP directory.
Maximum Number of Custom Contacts	Enter the maximum number of custom contacts that agents can add to Phonebook in Agent Desktop.
Log Call History	Select the **Log Call History** check box so that calls made by agents are logged. Agents can view the call history in the **Call History** tab of Phonebook in Agent Desktop.
Allow Erasing of Call History	Select the **Allow Erasing of Call History** check box so that agents can erase the call history from the **Call History** tab of Phonebook in Agent Desktop.
Append Selected Auto Phrase to Existing Text	Select the **Append Selected Auto Phrase to Existing Text** check box so that agents can add an automatic phrase to an existing chat message, IM message, or email message.
Allow Agent Desktop Panel Swap	Select the **Allow Agent Desktop Panel Swap** check box so that agents can move the **Left Pane** of Agent Desktop to the right side of Agent Desktop and vice-versa.
Autostart Quality of Service Window Service	Select the **Autostart Quality of Service Window Service** check box so that the Quality of Service (QoS) service automatically starts. **Note:** This is only applicable to Avaya Aura® environments, where embedded softphone is used in My Computer mode.
Enable AAAD System Tray Icon	Select the **Enable AAAD System Tray Icon** check box so that agents can add the **Avaya Aura Agent Desktop** system tray icon to the Windows system tray.
Enable AAAD Dashboard	Select the **Enable AAAD Dashboard** check box so that agents can collect and upload log files or videos to the CCMM server. Agents can also use the Dashboard to check the connectivity of Agent Desktop with the Contact Center servers. **Note:** By default, **Enable AAAD Dashboard** is selected in the CCMM Administration utility.

Table continues…

Name	Description
Prompt User for Login Details	Select the **Prompt User for Login Details** check box to automatically prompt agents to enter their credentials when Agent Desktop opens. If you do not select **Prompt User for Login Details** Agent Desktop tries to log in the agent using the current windows user credentials. If this login fails, Agent Desktop prompts the user to enter a set of credentials. **Important:** In an integrated AACC and POM solution, you must select the **Prompt User for Login Details** check box.
Disallow Duplicate Login	Select the **Disallow Duplicate Login** check box to prevent Agent Desktop from opening if the specified user ID is already logged into Contact Center from a different location.
Enable AAAD Preference Retention	Select the **Enable AAAD Preference Retention** check box to retain Agent Desktop preferences of the agents when agents log out of Agent Desktop and log back into Agent Desktop.
Enable Localization	Select the **Enable Localization** check box to turn on localization of Agent Desktop when a supported locale is detected on the client PC.
Default Not Ready Reason Code when Rejecting a Contact	Enter the default Not Ready Reason code that the system sends when an agent is forced into the Not Ready state after rejecting a contact. If the **Default Not Ready Reason Code when Rejecting a Contact** field is blank the agent is forced into the Not Ready state with a Reject Contact Default Code (000).
Default Not Ready Reason Code when Pulling a Contact	Enter the default Not Ready Reason code that the system sends when an agent is forced into the Not Ready state after pulling a contact. If the **Default Not Ready Reason Code when Pulling a Contact** field is blank the agent is forced into the Not Ready state with a Pull Mode Default Code (0000).
Default Not Ready Reason Code After Max Open Duration	Enter the default Not Ready Reason code that the system sends when an agent is forced into the Not Ready state when a contact is open for longer than the **Maximum Open Duration** and the contact is recycled.

Table continues…

Name	Description
	The CCMM Administration utility does not allow the **Default Not Ready Reason Code After Max Open Duration** field to be left blank. By default, the agent is forced into the Not Ready state with a MaxOpen Default Code (000).
Home Page Enabled	Select the **Home Page Enabled** check box so that Agent Desktop displays the **Home Page** button on the Agent Desktop toolbar. Agents can use the **Home Page** button to reopen the Agent Desktop home page. The Agent Desktop home page displays a screen pop that contains a web URL that you configure to open when an agent starts Agent Desktop.
Home Page URL	Type the web URL of the Agent Desktop home page. The home page displays a screen pop that contains this web page when an agent starts Agent Desktop.
Home Page Name	Type the name of the home page that Agent Desktop displays when an agent starts Agent Desktop.
Close Multiple Contacts	Select the type of user that can close multiple contacts simultaneously from search results. You can select one of the following options: • Supervisor. Select **Supervisor** to allow supervisors to close multiple contacts. • Agent. Select **Agent** to allow agents to close multiple contacts. This is the default option. • None. Select **None** so that no user has the permission to close multiple contacts.
Maximum Number of Calls to Log	Enter the maximum number of calls for which the call history is logged. Agents view the call history in the **Call History** tab of Phonebook in Agent Desktop.
Maximum Number of Speed Dials	Enter the maximum number of contacts that agents can add to their speed dial list in Phonebook.
Maximum Number of Favorites	Enter the maximum number of contacts that agents can add as favorites in Phonebook.
Contact Lookup Priority	Enter the order by which the system performs the caller name lookup. You can select one of the following options: • Custom contacts. Select **Custom contacts** so that the system performs caller name lookup from within the agent's custom contacts.

Table continues…

Name	Description
	• LDAP contacts. Select **LDAP contacts** so that the system performs caller name lookup from within LDAP contacts. • Intrinsics / Call property. Select **Intrinsics / Call property** so that the system performs caller name lookup by using the name taken from either an intrinsic property or a property on the call object. When a name matches the number on the incoming call, Agent Desktop displays that name on the user interface.
Insert Line Break Before Auto Response	Select the **Insert Line Break Before Auto Response** check box to add a blank line before an auto response is sent to the customer.
Display Agent Time in Not Ready State	Select the **Display Agent Time in Not Ready State** check box to display a timer on Agent Desktop that displays the duration the agent is in the Not Ready state.
Display Softphone Out Of Service Message on Start-up	Select the **Display Softphone Out Of Service Message on Start-up** check box to display a message box alerting agents that the CTI Link to the softphone is out of service while starting Agent Desktop in applicable configurations. The system also displays a message box to alert the agent that the softphone is now in service, after agents log using My Computer mode.
Show Original Action When Pulling MM Contact	Select the **Show Original Action When Pulling MM Contact** check box so that Agent Desktop displays the original action when pulling a contact. If you do not select the **Show Original Action When Pulling MM Contact** check box then Agent Desktop displays the most recent action when pulling a contact. An example of an original action is an email message that is sent by a customer. The most recent action is an agent's reply to the original email message.
Pop Up Notification – Closes After Time	This field is for Avaya Contact Center Select solutions only.
Pop Up Notification – Display Time	This field is for Avaya Contact Center Select solutions only.
Teleworker Recovery Button – Click Delay	This field is for Avaya Contact Center Select solutions only.

Table continues…

Name	Description
Bring AAAD to Front when Max Open Duration Exceeded	Select the **Bring AAAD to Front when Max Open Duration Exceeded** check box to automatically bring Agent Desktop to the front of the windows desktop when the contact is open for longer than the **Max Open Duration**.
Display Disposition Codes Names	Select the **Display Disposition Codes Names** check box so that Agent Desktop uses the **DisplayName** field to display disposition codes. By default, Agent Desktop uses the **Name** field to display disposition codes. Outbound Campaign Management Tool uses the **DisplayName** field to display disposition codes.
Show Web Comms System Prompts	Select the **Show Web Comms System Prompts** check box to display a message when an agent pushes a page to a customer. This message precedes the page push URL.
Use call attached data for skillset information	Select the **Use call attached data for skillset information** check box to display call attached data instead of the skillset intrinsic on contacts in Agent Desktop for AML-based contact centers.
Notify an Agent if a Contact is being Observed/ Barged-In On	Select the **Notify an Agent if a Contact is being Observed/Barged-In On** check box, so that Agent Desktop displays an icon on a work item when a supervisor/agent observes, whisper coaches, or barges-in on a call.
Display Observable Contacts of Logged Out Agents (SIP-enabled Contact Center only)	Select the **Display Observable Contacts of Logged Out Agents** check box to allow supervisor/ agents to see non-skillset calls of agents who are logged out of Agent Desktop. Supervisor/agents can see agent calls only where the agent uses CCT to log on to the desk phone.
Display Supervisor Observe Color Coding	Select the **Display Supervisor Observe Color Coding** check box, so that Agent Desktop uses color coding on the **Supervisor Observe** dialog to distinguish between skillset, non-skillset, observed, barged-in, and whisper coached calls and contacts.
Suppress OS softphone not supported popup	Select the **Suppress OS softphone not supported popup** check box to suppress a warning message that the softphone process is not supported on the Operating System on which Agent Desktop is running. By default, the **Suppress OS softphone not supported popup** option is not selected.

Table continues…

Name	Description
Enable one click copy of caller line ID (SIP-enabled Contact Center only)	Select the **Enable one click copy of caller line ID** check box to allow agents to use the **Copy CLID** button on the Agent Desktop toolbar to copy the Calling Line Identification (CLID) number of a customer to the clipboard. Agent Desktop displays the name of the caller using the contacts directory integration.
Maximum signature image file size	Enter a number that specifies the maximum file size for images that agents can add when creating a signature in Agent Desktop. Administrators can specify a value between 1 and 50 KB.
Maximum Number of Images Allowed Per Signature	Enter a number that specifies the maximum number of images that agents can add when creating a signature in Agent Desktop. Administrators can specify a value between 0 and 3. The default value is 3.
Maximum number of characters Per Email Signature	Enter a number that specifies the maximum number of characters that agents can add when creating a signature in Agent Desktop. Administrators can specify a value between 0 and 2000. The default value is 2000.
Force all agents to use a not ready reason code when going not ready	Select the **Force all agents to use a not ready reason code when going not ready** check box to force agents and supervisor/agents to enter a Not Ready reason code when agents change their status to Not Ready.
Display Previous Login Time	Select the **Display Previous Login Time** check box so that Agent Desktop displays the previous login time for the currently logged in agent. The login time displayed is the time of the CCT server and not the local time of the agent.
Show agent comments for external transfer	Select the **Show agent comments for external transfer** check box so that agent comments are added to an email that is transferred externally. By default, the **Show agent comments for external transfer** option is not selected.
Put Call on Hold During Transfer/Conference for the Enter Value	Select the **Put Call on Hold During Transfer/ Conference for the Enter Value** check box to place the customer call on hold when an agent initiates a call transfer or conference by entering the number in Agent Desktop.
Critical level of free Virtual Memory in MB	Enter the minimum amount of free RAM in MB that must be present on a client PC. If the free RAM drops below the level specified, Agent Desktop

Table continues…

Name	Description
	displays a warning message. By default, the minimum amount of free RAM is set at 250 MB.
Suppress OS not supported popup	Select the **Suppress OS not supported popup** check box to support Agent Desktop on Citrix. This is required for desktop virtualization.
Supported attachment file extensions	Configure the supported file extensions that agents can attach to emails in the **Supported attachment file extensions** field. For information on configuring the supported file extensions, see Restricting file extensions for attachments on page 386.
POM Custom fields sort order	Select the type of sorting that Agent Desktop performs on the custom fields for POM contacts. There are three options: • NO SORT: Agent Desktop displays the custom fields for POM contacts in the same order as received from the POM server. This is the default option. • ASC.: Agent Desktop displays the custom fields for POM contacts in an ascending order. • DESC.: Agent Desktop displays the custom fields for POM contacts in an descending order.

Configuring User Settings in a voice-only solution

About this task

The User Settings page contains configuration settings that you can customize for the Agent Desktop in a voice-only solution.

Procedure

1. Open the Multimedia Administration utility. See Starting the CCMM Administration utility on page 224.
2. In the left pane, select **Agent Desktop Configuration**.
3. Click **User Settings**.
4. Update the required settings.
5. Click **Save**.

Variable definitions

Name	Description
Display Customer History on Voice Contact	Select the **Display Customer History on Voice Contact** check box to display customer history for voice contacts on Agent Desktop. Contact Center Multimedia searches for customer history of previous contacts based on the calling line ID for voice contacts.
Display Customer History on Personal Calls (SIP-enabled Contact Center only)	Select the **Display Customer History on Personal Calls** check box to display customer history for voice contacts on personal calls on Agent Desktop.
Voice Contact Identifier for Customer History (SIP-enabled Contact Center only)	Select either **AD_CLID** or **SIP_FROM_ADDRESS** to look up the Contact Center Multimedia database that contains customer history for the originator of the incoming voice call. In order to search the database you must also enable the Voice Contact Search parameter.
Encoding Page of CCT Attached Data	Enter the value that determines the decode Code Page used to convert the Binary Attached Data stream to a String contact types for the configured intrinsics. This is used to retrieve the Skillset Name in an AML Contact Center. The system supports the following cases: • The default encoding, that is, the encoding specified in the regional settings for the computer executing this method • little-endian Unicode (UTF-16LE) • big-endian Unicode (UTF-16BE) • Windows operating system (windows-1252) • UTF-7 • UTF-8 • ASCII • Latin1 • GB18030 (Chinese Simplified) • CodePage Name • 1200 “UTF-16LE”, “utf-16”, “ucs-2”, “unicode”, or “ISO-10646-UCS-2” • 1201 “UTF-16BE” or “unicodeFFFE”

Table continues…

Name	Description
	• 1252 “windows-1252” • 65000 “utf-7”, “csUnicode11UTF7”, “unicode-1-1-utf-7”, “unicode-2-0-utf-7”, “x-unicode-1-1-utf-7”, or “x-unicode-2-0-utf-7” • 65001 “utf-8”, “unicode-1-1-utf-8”, “unicode-2-0-utf-8”, “x-unicode-1-1-utf-8”, or “x-unicode-2-0-utf-8” • 20127 “us-ascii”, “us”, “ascii”, “ANSI_X3.4-1968”, “ANSI_X3.4-1986”, “cp367”, “csASCII”, “IBM367”, “iso-ir-6”, “ISO646-US”, or “ISO_646.irv:1991” • 54936 “GB18030”
Suppress Browser Script Errors	Select the **Suppress Browser Script Errors** check box to suppress browser script errors.
Display Not Ready Reason Text Only	Select the **Display Not Ready Reason Text Only** check box to display only not ready reason text.
Display Voice Calls in Customer History	Select the **Display Voice Calls in Customer History** check box to display previous voice calls for the originator of the current active contact in Agent Desktop. Enable this setting to lookup the Contact Center Manager Server database for Voice Contact history. Enable **Contact Summary Data generation** in Contact Center Manager Administration, to ensure that individual contact history data is created in the Contact Center Manager Server database.
Audible Alert Setting	Select the type of alert Agent Desktop plays when contacts are presented to agents. There are four options: • NONE. No alert is played. • BEEP. The agents internal sound card is played as the alert. • WAV. A .wav audio file is played as the alert. • BOTH. Both the WAV and BEEP settings work.
Play Alert on Voice	Select the **Play Alert on Voice** check box to ensure an alert is played when voice contacts are presented to agents.
Source of WAV	Select MM or SPARK. This determines whether the .wav file played is a CCMM .wav file or the .wav file from Agent Desktop's Spark Emulator.
Display Caller's Friendly Name	In a SIP-enabled contact center, select the **Display Caller's Friendly Name** check box to enable a

Table continues…

Name	Description
	friendly name display on Agent Desktop for DN calls. When this is enabled, when one contact center agent receives a call from another contact center agent, the name of the calling agent (as configured in CCMA) displays on the Agent Desktop of the called agent. If a contact center agent receives a CDN call from another contact center agent, the friendly name displayed on the Agent Desktop of the called agent is the name of the calling agent as configured on the Avaya Aura® Communication Manager. **Note:** Both agents must be configured in CCMA for the friendly name to be displayed on Agent Desktop.
Highlight DN Call During Transfer	Determines which leg of the call has focus in Agent Desktop during a supervised transfer scenario, the original customer leg or the DN leg to the transfer party. Select the **Highlight DN Call During Transfer** check box to focus the DN leg to the transfer party in Agent Desktop during a supervised transfer scenario.
Put Call on Hold During Transfer for the Phonebook	Select the **Put Call on Hold During Transfer for the Phonebook** check box to place the customer call on hold when an agent initiates a call transfer, using the Phonebook on Agent Desktop.
Observe Agent Initiated Contact Center Calls (SIP-enabled Contact Center only)	Select the **Observe Agent Initiated Contact Center Calls** check box to allow agent-supervisors to use the Observe function to listen in on an agent-initiated voice contact.
Clear Previous Phone Number	Select the **Clear Previous Phone Number** check box to clear the number of the previous voice contact present on Agent Desktop.
Web Stats Ticker Duration	Enter the time, in seconds, for which the Web Statistics ticker displays for each skillset. **Note:** By default, the Web Statistics ticker displays for 10 seconds for each skillset on Agent Desktop.
Display Agent Login Duration	Select the **Display Agent Login Duration** check box to display the time that the agent is logged into Agent Desktop.

Table continues…

Name	Description
Pull Contact On Same Skillset Only	Select the **Pull Contact On Same Skillset Only** check box so that agents can pull contacts only from the skillsets that the agents are currently assigned to.
Web Stats Refresh Interval	Enter the time in seconds after which the Web Statistics information refreshes. **Note:** By default, the Web Statistics information refreshes every 60 seconds.
Web Stats Exception Limit	Enter the number of Contact Center Web Statistics (CCWS) connection exceptions allowed before the system disables the statistics feature. **Note:** If you enter zero in the **Web Stats Exception Limit** field, the statistics feature is never disabled.
Number of Rings on Voice Alert	Enter the number of times the agent phone rings when a voice contact alerts on Agent Desktop. **Note:** By default, the agent phone rings 5 times when a voice contact alerts on Agent Desktop.
Force Logout Delay	Enter the time, in seconds, the system displays the `You've Been Logged Out` alert before shutting down Agent Desktop, after a supervisor remotely logs an agent out of Contact Center from the Contact Center Manager Administration (CCMA) user interface. **Note:** By default, the system displays the `You've Been Logged Out` alert for 60 seconds.
Display System Defined Contact Center Codes	Select the **Display System Defined Contact Center Codes** check box so that Agent Desktop displays system-defined Not Ready Reason Codes and After Call Work Item codes.
Contact Center Code Display Preference	Select how Agent Desktop displays Contact Center codes. You can choose from the following: • Code. Agent Desktop displays Contact Center codes based on the code number. • Text. Agent Desktop displays Contact Center codes based on the code text.

Table continues…

Name	Description
	• Both. Agent Desktop displays Contact Center codes based on both the code number and the code text. **Note:** You can select **Contact Center Code Display Preference** only if you select the **Display System Defined Contact Center Codes** check box.
Enable Keyboard Shortcuts	Select the **Enable Keyboard Shortcuts** check box so that shortcut keys are enabled in Agent Desktop, and agents can use shortcut keys to perform common tasks on Agent Desktop. **Note:** By default, **Enable Keyboard Shortcuts** is selected in the CCMM Administration utility.
Allow Custom Contacts	Select the **Allow Custom Contacts** check box so that agents can add custom contacts to Phonebook in Agent Desktop. Custom contacts are personal contacts of the agents and are not present in the LDAP directory.
Maximum Number of Custom Contacts	Enter the maximum number of custom contacts that agents can add to Phonebook in Agent Desktop.
Log Call History	Select the **Log Call History** check box so that calls made by agents are logged. Agents can view the call history in the **Call History** tab of Phonebook in Agent Desktop.
Allow Erasing of Call History	Select the **Allow Erasing of Call History** check box so that agents can erase the call history from the **Call History** tab of Phonebook in Agent Desktop.
Allow Agent Desktop Panel Swap	Select the **Allow Agent Desktop Panel Swap** check box so that agents can move the **Left Pane** of Agent Desktop to the right side of Agent Desktop and vice-versa.
Autostart Quality of Service Window Service	Select the **Autostart Quality of Service Window Service** check box so that the Quality of Service (QoS) service automatically starts. **Note:** This is only applicable to Avaya Aura® environments, where embedded softphone is used in My Computer mode.

Table continues…

Name	Description
Enable AAAD System Tray Icon	Select the **Enable AAAD System Tray Icon** check box so that agents can add the **Avaya Aura Agent Desktop** system tray icon to the Windows system tray.
Enable AAAD Dashboard	Select the **Enable AAAD Dashboard** check box so that agents can collect and upload log files or videos to the CCMM server. Agents can also use the Dashboard to check the connectivity of Agent Desktop with the Contact Center servers. **Note:** By default, **Enable AAAD Dashboard** is selected in the CCMM Administration utility.
Prompt User for Login Details	Select the **Prompt User for Login Details** check box to automatically prompt agents to enter their credentials when Agent Desktop opens. If you do not select **Prompt User for Login Details** Agent Desktop tries to log in the agent using the current windows user credentials. If this login fails, Agent Desktop prompts the user to enter a set of credentials. **Important:** In an integrated AACC and POM solution, you must select the **Prompt User for Login Details** check box.
Disallow Duplicate Login	Select the **Disallow Duplicate Login** check box to prevent Agent Desktop from opening if the specified user ID is already logged into Contact Center from a different location.
Enable AAAD Preference Retention	Select the **Enable AAAD Preference Retention** check box to retain Agent Desktop preferences of the agents when agents log out of Agent Desktop and log back into Agent Desktop.
Enable Localization	Select the **Enable Localization** check box to turn on localization of Agent Desktop when a supported locale is detected on the client PC.
Default Not Ready Reason Code when Rejecting a Contact	Enter the default Not Ready Reason code that the system sends when an agent is forced into the Not Ready state after rejecting a contact. If the **Default Not Ready Reason Code when Rejecting a Contact** field is blank the agent is forced into the Not Ready state with a Reject Contact Default Code (000).

Table continues…

Name	Description
Default Not Ready Reason Code when Pulling a Contact	Enter the default Not Ready Reason code that the system sends when an agent is forced into the Not Ready state after pulling a contact. If the **Default Not Ready Reason Code when Pulling a Contact** field is blank the agent is forced into the Not Ready state with a Pull Mode Default Code (0000).
Default Not Ready Reason Code After Max Open Duration	Enter the default Not Ready Reason code that the system sends when an agent is forced into the Not Ready state when a contact is open for longer than the **Maximum Open Duration** and the contact is recycled. The CCMM Administration utility does not allow the **Default Not Ready Reason Code After Max Open Duration** field to be left blank. By default, the agent is forced into the Not Ready state with a MaxOpen Default Code (000).
Home Page Enabled	Select the **Home Page Enabled** check box so that Agent Desktop displays the **Home Page** button on the Agent Desktop toolbar. Agents can use the **Home Page** button to reopen the Agent Desktop home page. The Agent Desktop home page displays a screen pop that contains a web URL that you configure to open when an agent starts Agent Desktop.
Home Page URL	Type the web URL of the Agent Desktop home page. The home page displays a screen pop that contains this web page when an agent starts Agent Desktop.
Home Page Name	Type the name of the home page that Agent Desktop displays when an agent starts Agent Desktop.
Close Multiple Contacts	Select the type of user that can close multiple contacts simultaneously from search results. You can select one of the following options: • Supervisor. Select **Supervisor** to allow supervisors to close multiple contacts. • Agent. Select **Agent** to allow agents to close multiple contacts. This is the default option. • None. Select **None** so that no user has the permission to close multiple contacts.
Maximum Number of Calls to Log	Enter the maximum number of calls for which the call history is logged. Agents view the call history in

Table continues…

Name	Description
	the **Call History** tab of Phonebook in Agent Desktop.
Maximum Number of Speed Dials	Enter the maximum number of contacts that agents can add to their speed dial list in Phonebook.
Maximum Number of Favorites	Enter the maximum number of contacts that agents can add as favorites in Phonebook.
Contact Lookup Priority	Enter the order by which the system performs the caller name lookup. You can select one of the following options: • Custom contacts. Select **Custom contacts** so that the system performs caller name lookup from within the agent's custom contacts. • LDAP contacts. Select **LDAP contacts** so that the system performs caller name lookup from within LDAP contacts. • Intrinsics / Call property. Select **Intrinsics / Call property** so that the system performs caller name lookup by using the name taken from either an intrinsic property or a property on the call object. When a name matches the number on the incoming call, Agent Desktop displays that name on the user interface.
Display Agent Time in Not Ready State	Select the **Display Agent Time in Not Ready State** check box to display a timer on Agent Desktop that displays the duration the agent is in the Not Ready state.
Display Softphone Out Of Service Message on Start-up	Select the **Display Softphone Out Of Service Message on Start-up** check box to display a message box alerting agents that the CTI Link to the softphone is out of service while starting Agent Desktop in applicable configurations. The system also displays a message box to alert the agent that the softphone is now in service, after agents log using My Computer mode.
Bring AAAD to Front when Max Open Duration Exceeded	Select the **Bring AAAD to Front when Max Open Duration Exceeded** check box to automatically bring Agent Desktop to the front of the windows desktop when the contact is open for longer than the **Max Open Duration**.
Display Disposition Codes Names	Select the **Display Disposition Codes Names** check box so that Agent Desktop uses the **DisplayName** field to display disposition codes.

Table continues…

Name	Description
	By default, Agent Desktop uses the **Name** field to display disposition codes. Outbound Campaign Management Tool uses the **DisplayName** field to display disposition codes.
Use call attached data for skillset information	Select the **Use call attached data for skillset information** check box to display call attached data instead of the skillset intrinsic on contacts in Agent Desktop for AML-based contact centers.
Notify an Agent if a Contact is being Observed/ Barged-In On	Select the **Notify an Agent if a Contact is being Observed/Barged-In On** check box, so that Agent Desktop displays an icon on a work item when a supervisor/agent observes, whisper coaches, or barges-in on a call.
Display Observable Contacts of Logged Out Agents (SIP-enabled Contact Center only)	Select the **Display Observable Contacts of Logged Out Agents** check box to allow supervisor/ agents to see non-skillset calls of agents who are logged out of Agent Desktop. Supervisor/agents can see agent calls only where the agent uses CCT to log on to the desk phone.
Display Supervisor Observe Color Coding	Select the **Display Supervisor Observe Color Coding** check box, so that Agent Desktop uses color coding on the **Supervisor Observe** dialog to distinguish between skillset, non-skillset, observed, barged-in, and whisper coached calls and contacts.
Suppress OS softphone not supported popup	Select the **Suppress OS softphone not supported popup** check box to suppress a warning message that the softphone process is not supported on the Operating System on which Agent Desktop is running. By default, the **Suppress OS softphone not supported popup** option is not selected.
Enable one click copy of caller line ID (SIP-enabled Contact Center only)	Select the **Enable one click copy of caller line ID** check box to allow agents to use the **Copy CLID** button on the Agent Desktop toolbar to copy the Calling Line Identification (CLID) number of a customer to the clipboard. Agent Desktop displays the name of the caller using the contacts directory integration.
Force all agents to use a not ready reason code when going not ready	Select the **Force all agents to use a not ready reason code when going not ready** check box to force agents and supervisor/agents to enter a Not Ready reason code when agents change their status to Not Ready.
Display Previous Login Time	Select the **Display Previous Login Time** check box so that Agent Desktop displays the previous

Table continues…

Name	Description
	login time for the currently logged in agent. The login time displayed is the time of the CCT server and not the local time of the agent.
Put Call on Hold During Transfer/Conference for the Enter Value	Select the **Put Call on Hold During Transfer/ Conference for the Enter Value** check box to place the customer call on hold when an agent initiates a call transfer or conference by entering the number in Agent Desktop.
Critical level of free Virtual Memory in MB	Enter the minimum amount of free RAM in MB that must be present on a client PC. If the free RAM drops below the level specified, Agent Desktop displays a warning message. By default, the minimum amount of free RAM is set at 250 MB.
Suppress OS not supported popup	Select the **Suppress OS not supported popup** check box to support Agent Desktop on Citrix. This is required for desktop virtualization.
POM Custom fields sort order	Select the type of sorting that Agent Desktop performs on the custom fields for POM contacts. There are three options: • NO SORT: Agent Desktop displays the custom fields for POM contacts in the same order as received from the POM server. This is the default option. • ASC.: Agent Desktop displays the custom fields for POM contacts in an ascending order. • DESC.: Agent Desktop displays the custom fields for POM contacts in an descending order.

Configuring IIS to support MDB database file attachments in email messages

About this task

Configure Internet Information Services (IIS) to support Microsoft Access MDB files as attachments in Agent Desktop email messages. By default, IIS filters MDB file attachments.

Procedure

1. Log on to the CCMM server with administrative privileges.
2. On the **Desktop**, select **Administrative Tools**.
3. Select **Internet Information Services (IIS) Manager**.

4. In the left pane, navigate to the **Default Web Site**.
5. In the middle pane, in the **IIS** section, select **Request Filtering**.
6. From the **File Name Extensions** list, right-click **.mdb** and select **Remove**.
7. On the **Confirm Remove** message box, click **Yes**.
8. From the main **Internet Information Services (IIS) Manager** menu, select **File** > **Exit**.

Chapter 34: Data Management - cleanup and purging

Use the procedures in this chapter to set up the cleanup rules and scheduled tasks to archive closed contacts from the MULTIMEDIA database.

CCMM includes two databases for multimedia contacts, the MULTIMEDIA database and the OFFLINE database. The MULTIMEDIA database contains all active contacts. The OFFLINE database maintains an archive of contacts from the MULTIMEDIA database. This includes contacts both currently in and cleared from the MULTIMEDIA database.

A CCMM background offline synchronization task updates the OFFLINE database. You create rules and schedules to clean up the MULTIMEDIA database by removing closed contacts from it, while leaving them in the OFFLINE database. This keeps the MULTIMEDIA database small and efficient, while also allowing for historical reporting across all the contacts in both the active and the OFFLINE databases. You report on the OFFLINE database using custom reporting with an ODBC DSN referencing the Offline tables in the Multimedia namespace.

You can configure the OFFLINE database to purge contacts over a specific age. You specify the age at which AACC purges closed contacts. AACC runs a purge task every day, and purges contacts that meet the age criteria. You cannot recover a purged contact other than by restoring a backed-up OFFLINE database.

Database sizing and limits

The MULTIMEDIA database supports a maximum of 1,000,000 contacts. You must regularly cleanup contacts from the MULTIMEDIA database to stay below this limit. The maximum size of the OFFLINE database is 70% of the database drive size. For example, if the Multimedia database drive size is 200 GB, then the maximum size of the OFFLINE database is 140 GB. If the OFFLINE database fills up, you can either increase the Multimedia database disk space, or change the OFFLINE database purge interval.

To prevent service interruption, updates to the OFFLINE database stop when the database drive size is 70% full and the OFFLINE database has less than 5% free space. Updates continue after you purge contacts, or if space is freed or added to the drive.

You can check the current sizes of the databases in the CCMM Data Management tool.

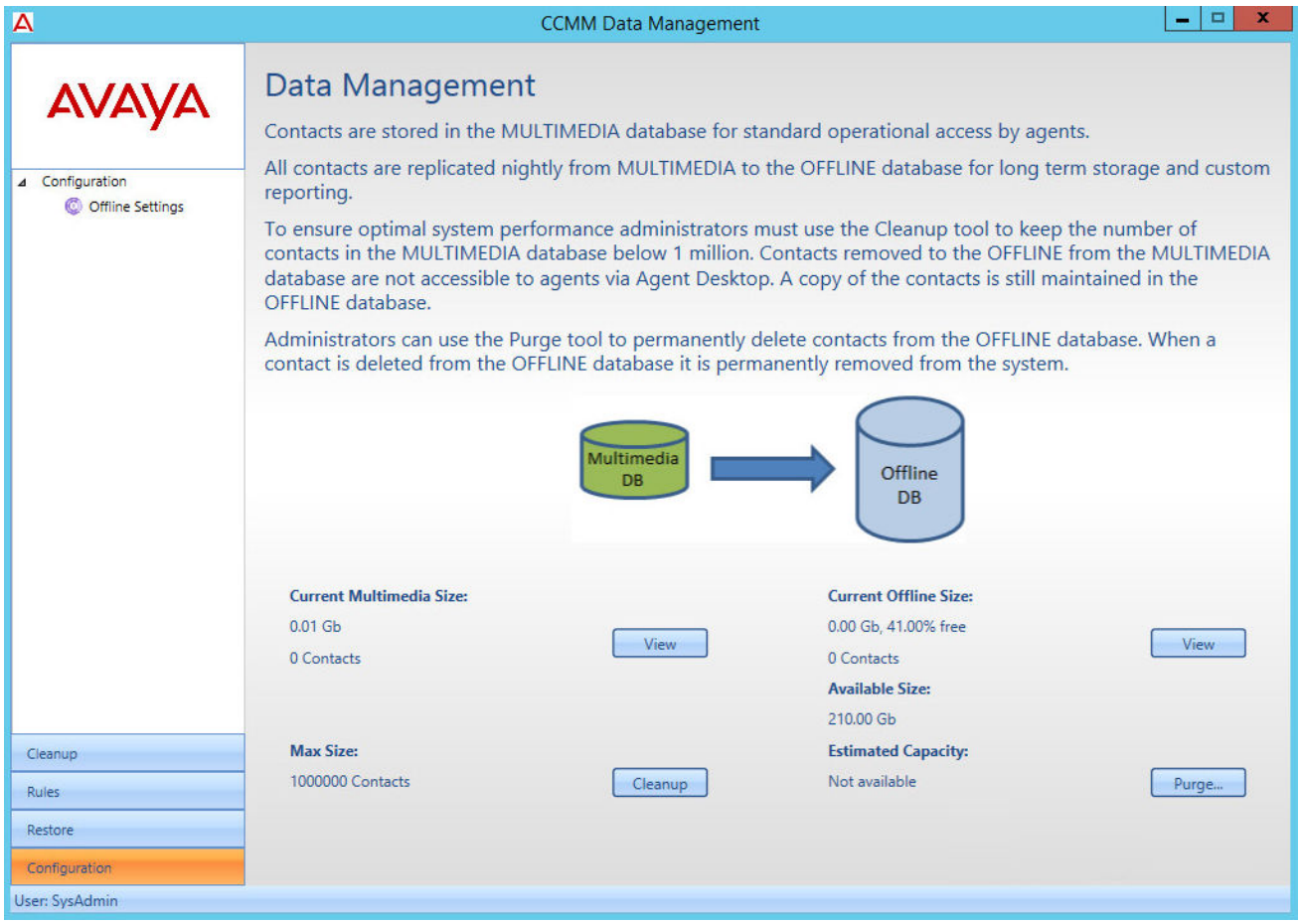


Figure 2: Data Management Configuration screen

When the current size of the OFFLINE database grows to 75% of the maximum size, CCMM logs this event to the log file. When the current size of the OFFLINE database grows above 90% of the maximum size, CCMM logs events to the event viewer. If the current size of the OFFLINE database exceeds 95%, CCMM stops automatically synchronizing contacts from the MULTIMEDIA database, and prevents you from running manual or scheduled cleanups.

You can configure purging of contacts from the OFFLINE database to reduce the database size. You specify the age at which AACC purges closed contacts. AACC runs a purge task every day, and purges contacts that meet the age criteria. You cannot recover a purged contact other than by restoring a backed-up OFFLINE database.

Cleanup rules

You create a cleanup rule to select contacts for a scheduled cleanup task. Cleanup rules apply to the MULTIMEDIA database only. Cleanup rules select contacts based on the number of days they have been in a Closed state, and any one of the following criteria:

- outbound campaign
- email rule
- contact skillset

- closed reason
- contact customer

In addition, there are four system cleanup rules:

- **Anonymous web customers with no contacts**: This rule clears anonymous customers that a Web Chat application can create, if it allows customers to start a web chat anonymously.
- **Customers with no contacts**: This rule clears customer records with no contacts, which can occur on systems upgraded from an earlier release.
- **All contacts more than 1 year old**: This rule clears all contacts that are more than 1 year old.
- **All contacts more than 5 years old**: This rule clears all contacts that are more than 5 years old.

You cannot modify these rules. They allow you to clear customer records with no contacts that occur in exceptional circumstances. Run scheduled tasks with these rules periodically to clear unwanted customer records from the active database.

Each scheduled cleanup task uses a rule, so you must create a rule before you can create a scheduled task.

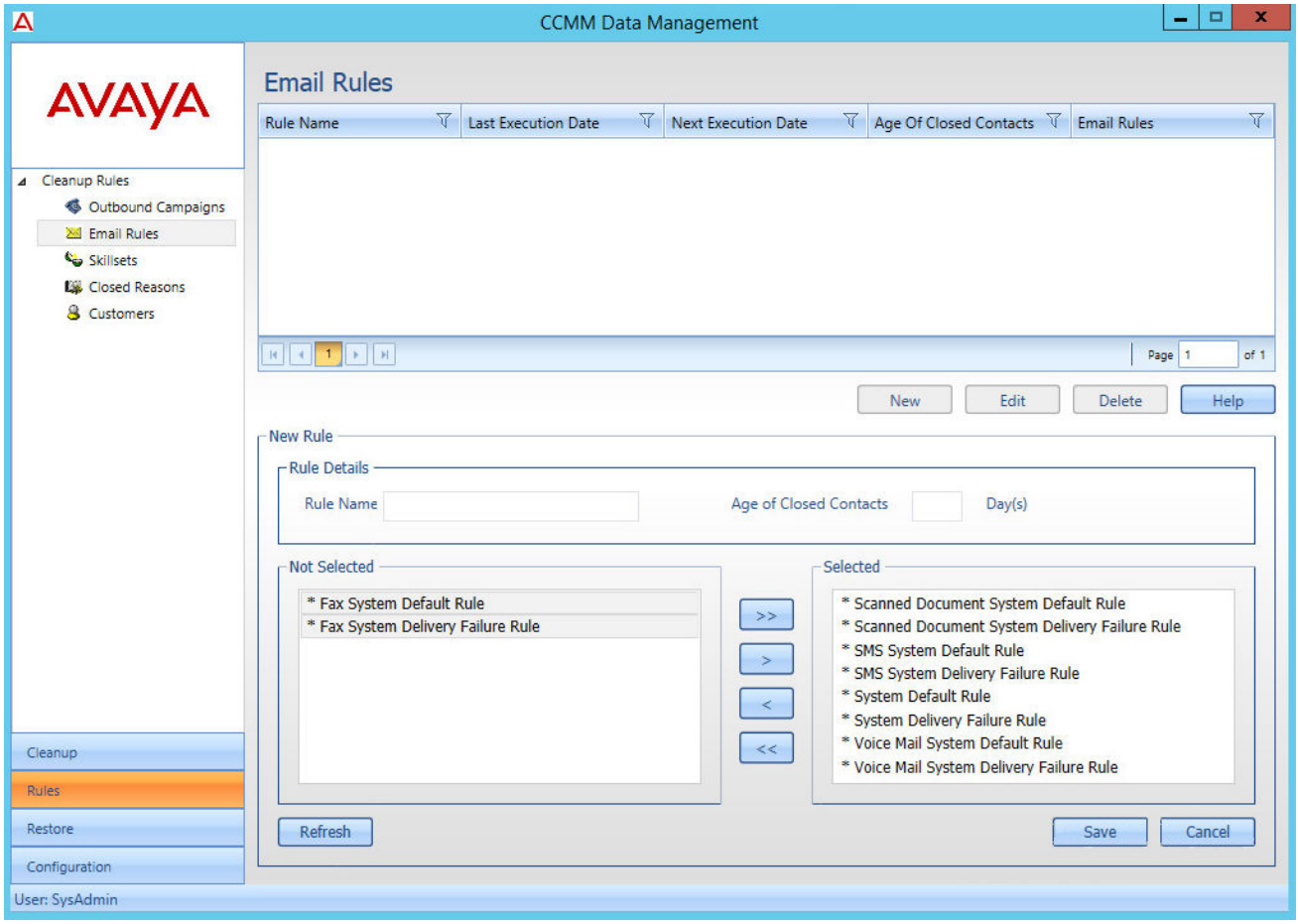


Figure 3: The Multimedia Data Management utility rules interface

Scheduled tasks

You create scheduled cleanup tasks to clear contacts from the MULTIMEDIA database. A scheduled task uses a single cleanup rule to select the contacts to clear. The scheduled task checks whether each contact matching the rule is archived in the OFFLINE database. If the contact is archived, the task clears it from the MULTIMEDIA database. If the contact is not archived, the cleanup task copies the contact to the OFFLINE database and then clears it from the MULTIMEDIA database.

The following figure shows the interface that you use to create scheduled cleanups of the MULTIMEDIA database.

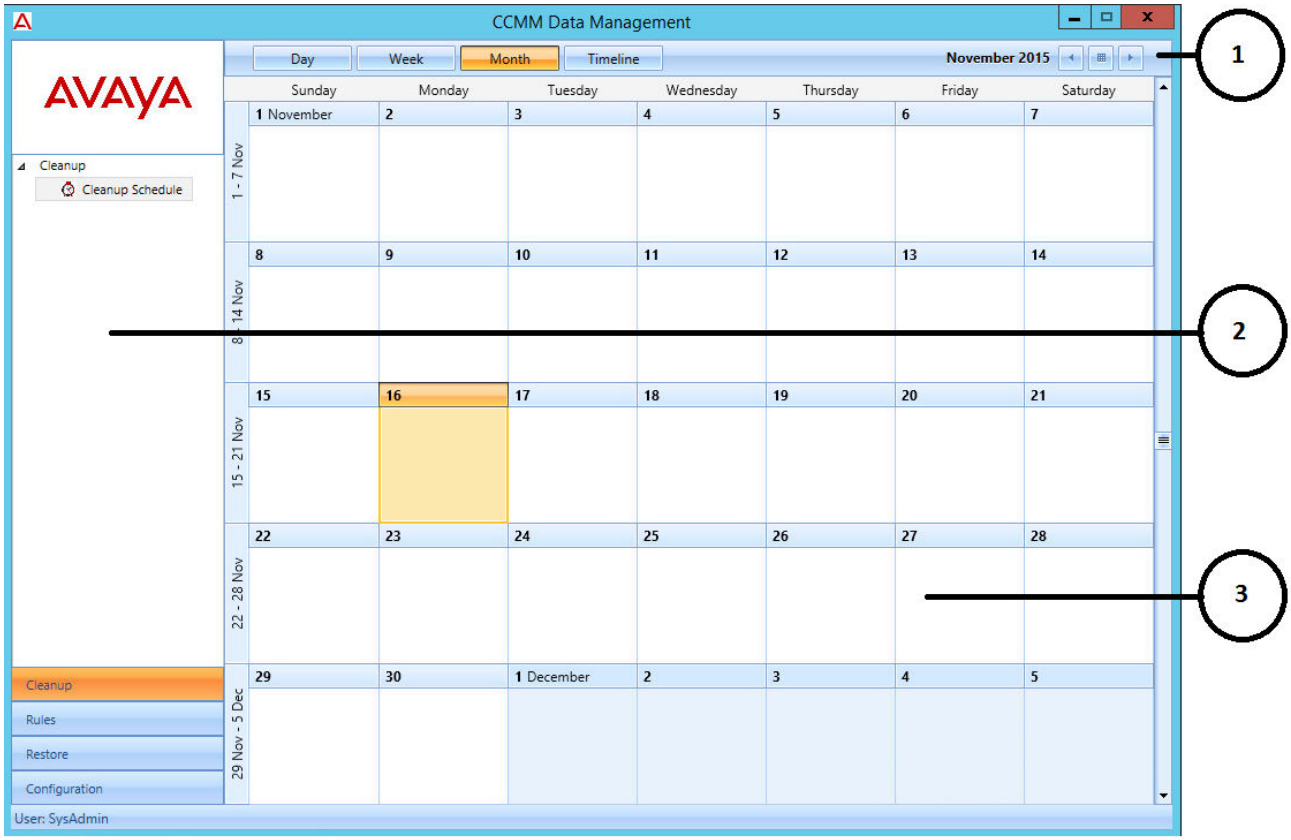


Figure 4: The Multimedia Data Management utility scheduling interface

The illustrated interface shows three work areas:

1	The Top Bar.
2	The Navigation Pane.
3	The Scheduled Task Calendar.

Restoring contacts

You can restore the contacts cleared by a scheduled cleanup task. For more information about restoring contacts, see *Maintaining Avaya Aura® Contact Center*.

Using the Multimedia Dashboard metrics to identify data to clean up

You can use the Multimedia Dashboard metrics to identify data to clean up. The CCMM Database Metrics section shows alerts when the metrics exceed normal thresholds. If you place your mouse over the alerting metric, the Dashboard displays a tooltip with details of the database values causing the alert. For example, if the database has one or more customers with over 1000 contacts, the tooltip displays:

- the customer IDs
- number of contacts for the customer

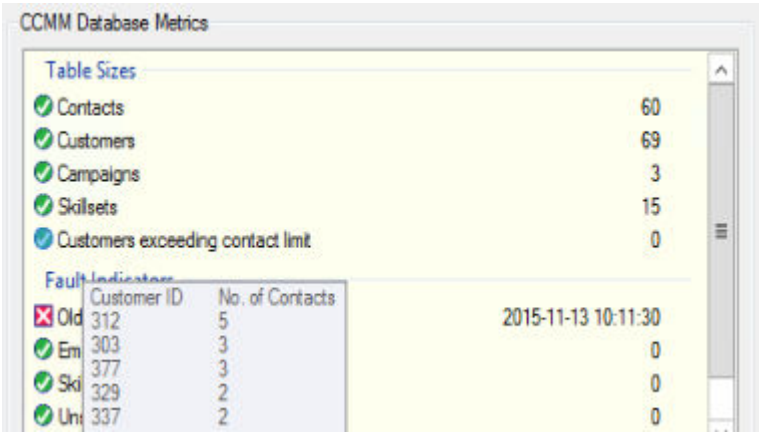


Figure 5: Example of a dashboard tooltip identifying the number of contacts customers have

Purging the OFFLINE Database

You can purge contacts from the OFFLINE database to reduce the database size. You cannot recover purged contacts, so it is important to back up the OFFLINE database before a purge. For more information about database backups and purging contacts, see *Maintaining Avaya Aura® Contact Center*.

Starting the Multimedia Data Management utility

Before you begin

- Log on to the Contact Center server.

About this task

Start the Multimedia Data Management utility to configure your cleanup rules and scheduled tasks.

Procedure

On the **Apps** screen, in the **Avaya** section, select **Data Management**.

Creating an Outbound Campaigns cleanup rule

Before you begin

- Log on to the Contact Center server.
- Start the Multimedia Data Management utility.

About this task

Create a cleanup rule to select closed contacts in the MULTIMEDIA database, based on the outbound campaign that closed the contact. You can use this rule in a scheduled cleanup task to clear these contacts from the MULTIMEDIA database. There are two criteria you can use to select contacts by outbound campaign:

- The number of days the contact has been in a Closed state.
- The outbound campaign that created and closed the contact.

Procedure

1. In the Data Management utility, select **Rules**.
2. Select **Outbound Campaigns**.
3. In the **Outbound Campaigns** screen, click **New**.
4. In the **Rule Name** field, enter a descriptive name for this rule.
5. In the **Age of Closed Contacts** field, type the number of days that a contact must be Closed to match this rule.
6. If you want to remove the campaign from the Outbound Campaign Management Tools (OCMT) Campaign List, select **Delete Campaign**.

   OCMT removes the campaign from the Campaign List when a cleanup task has removed all the campaign contacts and the campaign is Expired, Cancelled, or Completed.
7. For each campaign you want to add to the rule:
   a. In the **Not Selected** field, select an outbound campaign.
   b. Click the right-arrow button to move the outbound campaign to the **Selected** field.
8. For each campaign you want to remove from the rule:
   a. In the **Selected** field, select an outbound campaign.
   b. Click the left-arrow button to move the outbound campaign to the **Not Selected** field.
9. Click **Save**.

Next steps

Create a new scheduled task to use this rule to clear closed contacts from the MULTIMEDIA database.

Creating an Email Rules cleanup rule

Before you begin

- Log on to the Contact Center server.
- Start the Multimedia Data Management utility.

About this task

Create a cleanup rule to select closed email contacts in the MULTIMEDIA database. You can use this rule in a scheduled cleanup task to clear these contacts from the database. There are two criteria you can use to select email contacts:

- The number of days the contact has been in a Closed state.
- The email rule that the incoming email matched when Contact Center created the contact.

Procedure

1. In the Data Management utility, select **Rules**.
2. Select **Email Rules**.
3. In the **Email Rules** screen, click **New**.
4. In the **Rule Name** field, enter a descriptive name for this rule.
5. In the **Age of Closed Contacts** field, type the number of days that a contact must be Closed to match this rule.
6. For each email rule you want to add to the cleanup rule:
    a. In the **Not Selected** field, select an email rule.
    b. Click the right-arrow button to move the email rule to the **Selected** field.
7. For each email rule you want to remove from the rule:
    a. In the **Selected** field, select an email rule.
    b. Click the left-arrow button to move the email rule to the **Not Selected** field.
8. Click **Save**.

Next steps

Create a new scheduled task to use this rule to clear closed contacts from the MULTIMEDIA database.

Creating a Skillsets cleanup rule

Before you begin

- Log on to the Contact Center server.
- Start the Multimedia Data Management utility.

About this task

Create a cleanup rule to select closed contacts in the MULTIMEDIA database, based on the contact skillset. You can use this rule in a scheduled cleanup task to clear these contacts from the database. There are two criteria you can use to select contacts by skillset:

- The number of days the contact has been in a Closed state.
- The contact skillset.

Procedure

1. In the Data Management utility, select **Rules**.
2. Select **Skillsets**.
3. In the **Skillset Rules** screen, click **New**.
4. In the **Rule Name** field, enter a descriptive name for this rule.
5. In the **Age of Closed Contacts** field, type the number of days that a contact must be Closed to match this rule.
6. For each skillset you want to add to the cleanup rule:
    a. In the **Not Selected** field, select a skillset.
    b. Click the right-arrow button to move the skillset to the **Selected** field.
7. For each skillset you want to remove from the rule:
    a. In the **Selected** field, select a skillset.
    b. Click the left-arrow button to move the skillset to the **Not Selected** field.
8. Click **Save**.

Next steps

Create a new scheduled task to use this rule to clear closed contacts from the MULTIMEDIA database.

Creating a Closed Reason cleanup rule

Before you begin

- Log on to the Contact Center server.
- Start the Multimedia Data Management utility.

About this task

Create a cleanup rule to select closed contacts in the MULTIMEDIA database, based on the closed reason. You can use this rule in a scheduled cleanup task to clear these contacts from the database. There are two criteria you can use to select contacts by closed reason:

- The number of days the contact has been in a Closed state.

- The closed reason code an agent applied to the contact.

Procedure

1. In the Data Management utility, select **Rules**.
2. Select **Closed Reason**.
3. In the **Closed Reason Rules** screen, click **New**.
4. In the **Rule Name** field, enter a descriptive name for this rule.
5. In the **Age of Closed Contacts** field, type the number of days that a contact must be Closed to match this rule.
6. For each closed reason you want to add to the cleanup rule:
   a. In the **Not Selected** field, select a closed reason.
   b. Click the right-arrow button to move the closed reason to the **Selected** field.
7. For each closed reason you want to remove from the rule:
   a. In the **Selected** field, select a closed reason.
   b. Click the left-arrow button to move the closed reason to the **Not Selected** field.
8. Click **Save**.

Next steps

Create a new scheduled task to use this rule to clear closed contacts from the MULTIMEDIA database.

Creating a Customers cleanup rule

Before you begin

- Log on to the Contact Center server.
- Start the Multimedia Data Management utility.

About this task

Create a cleanup rule to select closed contacts in the MULTIMEDIA database, based on the contact customer. You can use this rule in a scheduled cleanup task to clear these contacts from the database. There are two criteria you can use to select contacts by customer:

- The number of days the contact has been in a Closed state.
- The contact customer.

Note:

The search function returns and displays the customer First and Last name. Different customers might share the same First and Last names. Therefore the results of the search function can be identical for different customer’s IDs.

Procedure

1. In the Data Management utility, select **Rules**.
2. Select **Customers**.
3. In the **Customer Rules** screen, click **New**.
4. In the **Rule Name** field, enter a descriptive name for this rule.
5. In the **Age of Closed Contacts** field, type the number of days that a contact must be Closed to match this rule.
6. For each customer you want to add to the cleanup rule:
    a. In the **Customer Search** field, select the search key for the customer, either **ID** or **E-mail**.
    b. In the **Equal To** field, type the ID or email address of the customer that you want to add to the rule.
    c. Click **Search**.
    d. Select the customer that the search function returns.
    e. Click the right-arrow button to move the customer to the **Selected** field.
7. For each customer you want to remove from the rule:
    a. In the **Selected** field, select a customer.
    b. Click the left-arrow button to move the customer to the **Not Selected** field.
8. Click **Save**.

Next steps

Create a new scheduled task to use this rule to clear closed contacts from the MULTIMEDIA database.

Creating a new scheduled cleanup task

Before you begin

- Log on to the Contact Center server.
- Start the Multimedia Data Management utility.
- Create a new rule to select the contacts you want to clear.

About this task

Create a scheduled cleanup task to clear contacts from the MULTIMEDIA contact database. A scheduled task uses a single cleanup rule to select the contacts to clear. Scheduled tasks clear only closed contacts that were already copied to the OFFLINE database. If a contact was not previously copied to the OFFLINE database, the scheduled task copies it before clearing it.

You can select only a single rule for each scheduled task. You can choose to run a scheduled task once, weekly, or monthly. If you select to run a scheduled task weekly or monthly, you can optionally set an end date after which the scheduled task does not run.

The Cleanup Schedule interface shows a calendar, in a similar manner to many graphical scheduling tools. You can change the calendar to use Week, Month, or Timeline views.

Procedure

1. In the Data Management utility, select **Cleanup**.
2. Select **Cleanup Schedule**.
3. In the schedule calendar, select the date on which you want to schedule a cleanup task. You can use the **Day**, **Week**, **Month**, **Timeline**, **Back**, **Calendar**, and **Forward** controls in the Top Bar to browse to a date if it is not currently visible.
4. Double click the date on which you want to create the scheduled task.

   Contact Center displays the **Schedule Cleanup** window.
5. In the **Name** field, enter a display name for this scheduled task.
6. In the **Description** field, enter a description of what this scheduled task does.
7. In the **Select Type** field, select the type of cleanup rule for this scheduled task.
8. In the **Select Rule** field, select an existing cleanup rule that the scheduled task uses to identify contacts to clear.
9. In the **Schedule** section, select the frequency with which you want this task to run; either **Run Once**, **Weekly**, or **Monthly**.
10. If you selected **Run Once**:

    In the **Start Date** fields, select the date and time on which you want the task to run.
11. If you selected **Weekly**:
    a. In the **Start Date** fields, select the first date and time on which you want the task to run.
    b. Select the days of the week on which you want the task to run.
    c. If you want this scheduled task to stop running after a date in the future, select **End on** and select a date after which this task does not run.
12. If you selected **Monthly**:
    a. In the **Start Date** fields, select the first date and time on which you want the task to run.
    b. In the **Day** field, enter the day of the month on which you want the task to run.
    c. In the **of every** field, enter the frequency of this monthly task.

       For example, enter 1 to run the task every month, enter 2 to run the task every second month, or enter 12 to run the task once a year.
    d. If you want this scheduled task to stop running after a date in the future, select **End on** and select a date after which this task does not run.

13. Click **Save**.

Enabling OFFLINE database purging

Before you begin

- Log on to the Contact Center server.
- Start the Multimedia Data Management utility.

About this task

Enable OFFLINE database purging to permanently remove closed contacts from the OFFLINE database. Choose the length of time that closed contacts can remain in the OFFLINE database before Contact Center purges them. Contact Center runs the purge task every day, and deletes contacts that have been closed for the duration you configure. Avaya recommends that you do not configure purging unless the OFFLINE database approaches maximum usage.

Important:

When Contact Center purges a contact from the OFFLINE database, you cannot recover the contact except by retrieving it from a backed-up OFFLINE database. Ensure the duration you configure to retain contacts is consistent with your local legislative and corporate data retention requirements.

Procedure

1. In the Data Management utility, select **Configuration**.
2. Click **Purge**.
3. On the **Purge Settings** dialog, select **Enable Data Purge**.
4. In the **Keep Offline records (months)** field, type the number of months a contact must be closed for Contact Center to purge it from the OFFLINE database.

   Ensure the value you enter is consistent with your local legislative and corporate data retention requirements.
5. Click **Save**.
6. On the **CCMM Data Management** dialog, click **Yes**.
7. On the **Purge Settings** dialog, click **Close**.

Restoring an archive from a previous Release

Before you begin

- The archive from the previous Release must be in the original archive location.

About this task

You can restore Multimedia database archives from the previous Release if you need to recover old contacts to work with them. Use the legacy Multimedia Archive/Restore Utility to restore the contacts. Reopen the contacts you want to work with, and then cleanup the rest of the contacts so that Contact Center moves them to the OFFLINE database.

Procedure

1. Run the legacy Multimedia RestoreArchive executable `D:\Avaya\Contact Center\Multimedia Server\Server Applications\ARCHIVE RESTORE\ArchiveRestore.exe`.
2. Click **Restore**.
3. In the **Restore** pane, select the archive you want to restore.
4. Click **Restore**.
5. When the restore completes, exit the Archive/Restore Utility.
6. Use Agent Desktop to search for and reopen the contacts that you want to work with, so that they remain in the MULTIMEDIA database.
7. On the **Apps** screen, in the **Avaya** section, select **Data Management**.
8. Create a new cleanup rule to clear the restored contacts from the active database. The configuration of this rule depends on the contacts that you restored.
9. Click **Cleanup Schedule**.
10. Create a scheduled task with the new cleanup rule to clear the restored contacts from the MULTIMEDIA database.

Chapter 35: Data Management - customer privacy

The Multimedia Data Management utility includes a Customer Privacy tab that allows you to act on privacy requests from contact center customers. The following customer privacy requests can be addressed using the Multimedia Data Management utility:

- If a customer exercises their right to access information, you can provide customers with information stored about them in the MULTIMEDIA and OFFLINE databases. You can save this information in an XML file, which can be modified before you provide it to the customer. The file contains all relevant customer information.
- If a customer exercises the right to be forgotten, you can delete their history records from the MULTIMEDIA and OFFLINE databases. In High Availability solutions, the records are also deleted from standby and RGN servers.

Note:

To prevent deletion of contacts not yet handled by agents, a customer's history records can be fully deleted only when all of their contacts are in a closed status. For example, a customer with contacts in new or open status cannot not be deleted.

Generating a customer information file

About this task

If you receive a customer information request, use the Multimedia Data Management utility to generate customer information in an XML file. You can then modify this file if required, before you provide it to the customer.

The Multimedia Data Management utility retrieves the customer information from the MULTIMEDIA and OFFLINE databases.

You can search for customers based on Customer ID or email address.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Data Management**.
2. In the Data Management utility, select **Privacy**.
3. Select **Information Request**.

4. Under **Customer Search**, from the drop-down list, select **ID** or **E-mail**.
5. In the **Equal To** box, type the customer's ID or email address and click **Search**.
6. Select the customer and click **Save As**.
7. Navigate to the folder where you want to save the XML file.
8. In the **File name** box, type a name for the file and click **Save**.
9. After the file saves, click **OK** on the dialog box confirming the file location.

Note:

The time it takes to generate the file depends on the size of the customer record.

Next steps

Modify the file if required before providing it to the customer.

Deleting customer history

About this task

If you receive a customer right to be forgotten request, use the Multimedia Data Management utility to delete customer history records from the MULTIMEDIA and OFFLINE databases.

You can search for customers based on Customer ID or email address.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Data Management**.
2. In the Data Management utility, select **Privacy**.
3. Select **Delete Request**.
4. Under **Customer Search**, from the drop-down list, select **ID** or **E-mail**.
5. In the **Equal To** box, type the customer's ID or email address and click **Search**.
6. Select the customer and click **Delete**.
7. Click **Yes** to confirm that you want to delete the customer history record.

Part 8: Avaya Aura® Media Server

- Avaya Aura Media Server configuration on page 436

Chapter 36: Avaya Aura® Media Server configuration

This section includes configuration procedures for Avaya Aura® Media Server in a SIP-enabled contact center. Avaya Aura® Contact Center uses the media processing capabilities of Avaya Aura® Media Server to support SIP-enabled contact centers.

Prerequisites to Avaya Aura® Media Server configuration

Procedure

Commission Avaya Aura® Media Server. For more information, see *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications*.

Logging on to Avaya Aura® Media Server Element Manager

Before you begin

- Obtain a valid user name and password to access Avaya Aura® Media Server (Avaya Aura® MS) Element Manager.

About this task

Log on to the Avaya Aura® Media Server Element Manager as an administrator to configure Avaya Aura® Media Server.

Element Manager (EM) is a web-based administration tool that facilitates the Operation, Administration, and Maintenance (OAM) of Avaya Aura® Media Server. A SIP-enabled Contact Center solution must contain one or more Avaya Aura® Media Server servers. Each Avaya Aura® Media Server server in the Contact Center solution must be licensed and configured to provide media services.

Procedure

1. On the Avaya Aura® Media Server server, start a Web browser.
2. In the address box, enter https://SERVER_IP_ADDRESS:8443/em. Where SERVER_IP_ADDRESS is the IP address of the Avaya Aura® Media Server.

3. In the **User ID** box, type the Avaya Aura® Media Server User ID logon account name. The default Element Manager User ID account name is *cust*.
4. In the **Password** box, type the Avaya Aura® Media Server Element Manager password. The default Element Manager password is the *cust* password.
5. Click **Sign In**.

Uploading a batch zip file

Before you begin

- Add the content namespace. For more information, see *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications*.
- Create the media files for a Content Namespace on your local system. You must organize the media files in the required file structure. Then zip the media files.

Important:

You must give the root directory the same name as the content namespace name.

About this task

You can upload a batch file to provision multiple media files on the Avaya Aura® Media Server in a single step. This can include all the media to provide call treatments such as announcements or music.

You can provision the media in a content namespace by using one ZIP file for the whole content namespace or by creating one content group at a time. After you upload the media file, Element Manager (EM) displays it in a tree view. The root of the tree is the content namespace and individual content groups appear below it. EM displays the content namespace and the content groups in the left pane, and the media files contained in the selected content group in the right pane.

Note:

If your solution has an Avaya Aura® Media Server cluster, perform this Content Store procedure only on the primary Avaya Aura® Media Server.

Note:

If your solution has a single Avaya Aura® Media Server High Availability pair, perform this Content Store procedure only on the primary Avaya Aura® Media Server. If your contact center solution has more than one Avaya Aura® Media Server High Availability pair, perform this Content Store procedure only on the Avaya Aura® Media Server High Availability Content Store master pair. Avaya Aura® Media Server High Availability Content Store replication duplicates this Content Namespace to all other Avaya Aura® Media Servers in your solution.

Procedure

1. Log on to Element Manager from the system on which you have created the batch zip file.
2. In the navigation pane, click **Tools** > **Media Management**.

3. On the **Media Management** page, select the check box next to the content namespace to which you want to add the media.
4. Click **Browse**.

   Avaya Aura® MS displays the Provision Media page.
5. On the **Provision Media** page, right-click the content namespace and select **Batch File Provision** on the shortcut menu.
6. On the **Batch File Provision** dialog box, click **Browse**, and then navigate to the zip file to upload.
7. Click **Always overwrite file with the same name**.

   OR

   Click **Do not overwrite files with the same name**.
8. Click **Upload**.

Configuring Avaya Aura® Media Server name resolution

About this task

Configure Avaya Aura® Media Server to resolve the hostname and Fully Qualified Domain Name (FQDN) of the Contact Center Manager Administration server. The Contact Center Manager Administration (CCMA) software is installed on the Contact Center server.

Procedure

1. Log on to Element Manager with administrative privileges.
2. Navigate to **EM** > **System Configuration** > **Network Settings** > **Name Resolution**.
3. Click **Add**.
4. In the **IP Address** box, enter the Contact Center Manager Administration IP address.
5. In the **Hostname** box, enter the Contact Center Manager Administration hostname.
6. Click **Save**.

Enabling SNMP traps

Before you begin

This procedure requires you to restart the Avaya Aura® MS server.

About this task

Avaya Aura® MS uses the Simple Network Management Protocol (SNMP) protocol to provide logs and events that need administrative attention to a central management system.

Avaya Aura® MS reports SNMP traps to the management system when corresponding events trigger. For example, Avaya Aura® MS reports an SNMP trap when Avaya Aura® MS logs a critical event.

Note:

By default, the SNMP service is disabled on Avaya Aura® MS.

If you want to integrate the Avaya Aura® MS management information base (MIB) into your SNMP infrastructure, you can find the MIB files in the following locations:

- on Windows: `%MASHOME%\MIB\AVMediaServer-smi2.mib`
- on Linux: `$MASHOME/MIB/AVMediaServer-smi2.mib`

Procedure

1. Open the Element Manager for Avaya Aura® MS.
2. In the navigation pane, click **System Configuration** > **Network Settings** > **General Settings** > **SNMP Traps**.
3. Select **SNMP Alarm Delivery Traps** and **SNMP Event Log Delivery Traps**.

   You can enable reporting of alarms to a management system by selecting **SNMP Alarm Delivery Traps**. You can enable reporting of events to a management system by selecting **SNMP Event Log Delivery Traps**.
4. In the **SNMP Network Manager Address** box, enter the address and the port number of the SNMP server that receives the reports.

   The format of the address and port number must be `address:port`. The default port number is 162.
5. Specify the community string shared with the SNMP management server in the **Community String** field.

   Note:

   The SNMP management server rejects reports that do not match the expected community string.
6. Click **Save**.
7. Restart the system.

Configuring the Avaya Aura® Media Server SNMP agent

Before you begin

This procedure requires you to restart the Avaya Aura® Media Server server.

About this task

Avaya Aura® Media Server uses the SNMP protocol to provide logs and events that need administrative attention to a central management system.

When the management system raises queries, the SNMP Agent on Avaya Aura® MS receives these queries and responds to the management system with the requested information.

Procedure

1. Open the Element Manager for Avaya Aura® Media Server.
2. In the navigation pane, click **System Configuration** > **Network Settings** > **General Settings** > **SNMP Agent**.
3. Specify the community string shared with the SNMP management server in the **Community String** field.

   Note:

   Avaya Aura® MS SNMP Agent rejects queries that do not match the expected community string.
4. Specify the SNMP Agent port number in the **Port Number** field.

   The default port number is 161.
5. Click **Save**.
6. Restart the system.

Configuring log filter settings

About this task

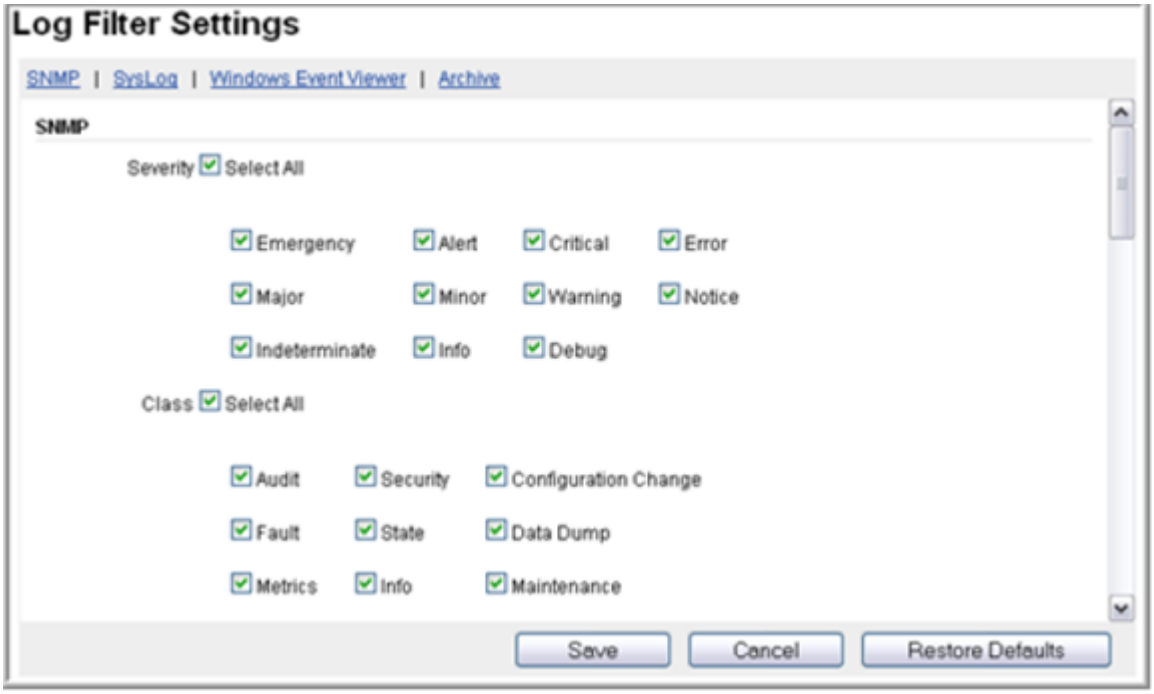
Each log destination you configure on Avaya Aura® MS, whether SNMP, SysLog, or Archive, has filter settings, which you can customize independently.

You can filter logs based on severity and class. Only those events that you select in the Log Filter Settings page are logged. For more information on filter options, see Procedure job aid on page 441.

Procedure

1. Open the Element Manager for Avaya Aura® MS.

2. In the navigation pane, click **System Configuration** > **Monitoring Settings** > **Event Logs** > **Log Filter Settings**.



3. Configure the filters for each destination: **SNMP**, **SysLog**, and **Archive**.
4. Click **Save**.

Procedure job aid

You can filter logs based on severity and class, as described in the following tables:

Table 3: Filter options by log severity

Event type	Description
Emergency	An unusable system.
Alert	An action must be taken immediately.
Critical	An immediate corrective action that is required due to loss of service, loss of bandwidth, outage, and loss of data or functionality.
Error	An error condition has occurred.
Major	An urgent corrective action that is required due to a pending loss of service, outage, and loss of data or functionality.
Minor	An urgent corrective action that is required due to a pending loss of service, outage, and loss of data or functionality.

Table continues…

Event type	Description
Warning	A potential or impending service-affecting condition that is detected that requires some diagnostic action.
Notice	A normal but significant condition.
Indeterminate	A service-affecting condition that is detected whose impact is unknown.
Info	Audit-type information and configuration changes.
Debug	Diagnostic information.

Table 4: Filter options by log class

Event type	Description
Audit	Audit events provide notification of very specific actions within a managed device. In isolation, an audit event provides limited data. However, a collection of audit information forms an audit trail.
Security	Audit events provide notification of very specific actions within a managed device. In isolation, an audit event provides limited data. However, a collection of audit information forms an audit trail.
Configuration Change	A configuration event, also known as an inventory event, is used to notify the system that hardware, software, or a service has been added, changed, or removed.
Fault	The system generates a fault notification after a fault condition occurs. A fault notification can result in an alarm.
State	A state includes both administrative states that can be manually configured and operational states that are read-only and determined by the managed entity.
Data Dump	A data dump event is an asynchronous event that contains information about a system, such as the configuration and the state. The system generates these events as a result of a scheduled activity. Data dump events are not intended for a traditional poll-response type interaction.
Metrics	A metrics event contains a metric or a collection of metrics, including performance metrics, for an application, platform, or another device or network element. The record can be in a number of different formats, for example, XML, CSV.
Info	An event of interest which requires no action but can be used for troubleshooting purposes.
Maintenance	A maintenance event signals the beginning, process, or end of an action generated either by a manual or an automated maintenance action. Typically, the system reports the actual action initiation and the maintenance action.

Part 9: Security Administration

- Security Fundamentals on page 444
- Contact Center security certificates administration on page 447
- Database encryption administration on page 470
- Windows Server 2012 security for Contact Center on page 474
- Avaya Aura Media Server security certificates administration on page 476

Chapter 37: Security Fundamentals

Secure Avaya Aura® Contact Center to enable the user to secure the different applications available.

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a protocol that provides a systematic way to monitor and manage a computer network. The SNMP model consists of four components:

- managed nodes, which can be any device (such as a host, a router, or printer), that is capable of communicating status to network-management systems through an SNMP management process called an SNMP Agent
- management stations, which can be computers running special network management software that interact with the Agents for status
- management information, which is conveyed through exact specifications and format of status specified by the MIB
- Management Protocol or SNMP, which sends messages called protocol data units (PDUs)

Event viewer settings

Events are log entries that record activities in the Contact Center suite of application servers, such as sending or receiving messages, opening or closing applications, and errors. Some events are for information only, while others can indicate problems. You can filter events by several categories, such as severity and event code range. You can also limit the display to the most recent events.

Event Severity

The system assigns one of the following severity levels to each event.

Information

These events indicate that something noteworthy happened on the system but do not indicate a problem. For example, an information-level event can indicate that a service started or stopped. These events appear in the Event Browser but not in the Alarm Monitor.

Minor

These events indicate that a non-service-affecting fault condition exists and that you must take corrective action to prevent a more serious fault. For example, a minor event is generated when the file system is 90 percent full.

Major

These events indicate that a condition exists which affects services and you must take corrective action. The event condition can cause severe degradation in server performance, and you must restore full capacity. For example, a major event is generated when the file system is 100 percent full.

Critical

These events indicate that a condition which affects services exists and you must immediately take corrective action. Critical events are reported when a component is completely out of service, and you must take immediate action to restore it. For example, a critical event is generated when the file system crashes.

Event Browser and Alarm Monitor

The Event Browser and Alarm Monitor show events that occur on the server. These programs provide many common features to view events.

You can configure the Alarm Monitor to automatically appear in the foreground of the desktop when an event occurs and you can specify whether the Alarm Monitor appears in the foreground for only critical events, major and critical events, or all events, or whether it stays in the background for all events.

In the Alarm Monitor, you can filter events by severity only. The Alarm Monitor does not display information events.

Contact Center Manager Server Utility to view events on CCMS

The Contact Center Manager Server Utility allows you to monitor and maintain Contact Center Manager Server. The Contact Center Manager Server Utility also provides functionality that is not available through Contact Center Manager Administration.

You can install Contact Center Manager Server Utility on a stand-alone computer, or it can co-reside with the Contact Center Manager Server. In a network, the Contact Center Manager Server Utility can co-reside with the Network Control Center Server.

Chapter 38: Contact Center security certificates administration

Contact Center includes a number of services and connections that you can secure using Transport Layer Security (TLS). You can install Contact Center with security enabled for commonly used Web services and CTI connections. You can use the Ignition Wizard to create a security store, generate a Certificate Signing Request (CSR) and import a Certificate Authority root certificate. Use the procedures in this chapter to administer Contact Center security, including turning off security, creating a new security store, and modifying the security store inspection task.

Modifying the Contact Center security certificates can impact many connections and services. The following connections and services use Contact Center security certificates to implement TLS:

- Application Enablement Services (AES) CTI call control
- Contact Center Manager Administration (CCMA)
- Contact Center Multimedia (CCMM) Administration
- Agent Desktop
- Multimedia Services
- Orchestration Designer
- Outbound Campaign Management Tool
- Agent Browser application
- Agent Greeting and Announcement Recorder

Contact Center security store

Contact Center includes a security store for Web services, to enable secure communications over TLS, both between Contact Center applications and with external clients or third party applications.

The Contact Center security store includes a server certificate and root certificate. Contact Center also uses the Internet Information Services (IIS) security store for some services. In addition, the Contact Center Open Interfaces have unique security stores.

Security Manager

Security Manager provides an interface for managing the security certificates in the Contact Center security store and the IIS security store. Contact Center supports the management of the IIS security store only through Security Manager: do not use IIS functions to manage the IIS security store on a Contact Center server. Security Manager supports importing chained certificates, and places these certificates in the Contact Center security store for distribution across the solution.

Supported TLS versions

Contact Center defaults to using only TLS 1.2 for secured services and connections. For backward compatibility, Contact Center supports Administrators changing the minimum TLS version that

Contact Center can negotiate with other systems. This is to inter-operate with legacy systems that do not support TLS 1.2. You can set minimum TLS versions separately for the following connections:

- SIP signaling
- CCMA and CCMM administration
- Event Broker Web service (this setting also sets the minimum TLS version used for Web Statistics)

If you change the CCMA and CCMM administration setting, the configuration applies the Windows Server 2012 TLS settings, and affects all applications on the server that use Windows Server 2012 secure communications technology.

When the Contact Center configuration is for a TLS version lower than 1.2, Contact Center still attempts to negotiate the highest (and most secure) version first, before stepping down to a lower (and less secure) version.

Avaya recommends that you maintain the TLS version settings at the highest possible TLS version, and that you change these settings only when it is certain that parts of your overall contact center solution do not work with the higher TLS version.

Contact Center High Availability

In a High Availability (HA) system, the security stores must use Subject Alternative Names (SANs). Include a SAN for the Managed name and the server name. This ensures clients connecting to Contact Center using the managed name do not get warnings that the signed certificate name does not match the server name.

Certificate Authority root certificates

When a client initiates a secure connection with a server, it must have a root certificate from the CA that provided the server signed certificate. If the client does not have a matching root certificate, it does not complete the connection. If the client has a root certificate from a CA, it can trust any server certificate signed by that CA.

Avaya recommends that you use a single CA to sign all the certificates in your contact center. This simplifies the deployment process, because you need to distribute only a single root certificate to all the clients. If you want to use different CAs to sign certificates for your different servers, you must copy the root certificate from each CA to all the clients in your contact center.

For some Web services, servers can act as clients of other servers. Therefore you must ensure that all servers also have the required CA root certificate(s).

Offline Store

You can create an offline store using Security Manager, which minimizes downtime if you want to replace your current security store. When your offline store is created, you can swap between the active store and the offline store. You can make the offline store the active store at any point using Security Manager. You must stop Contact Center services before making the offline store active.

Security Store notifications

Security certificates contain an expiration date and they are not valid after this date. If the security certificates used by Contact Center expire, the contact center loses call control and stops functioning.

Security Manager provides a security store inspection utility to help you monitor and maintain valid security certificates. You can use Security Manager to schedule a security store inspection task.

Security Manager adds the scheduled task to the underlying Windows Task Scheduler. The scheduled task runs the security store inspection utility once a week. The inspection utility checks the status of the security certificates in the Contact Center security store. If any of the security certificates are due to expire within a month, the inspection utility sends a notification email to the contact center administrator. The contact center administrator must then refresh the security certificates.

Security Manager provides the notification email; it cannot renew expired security certificates. For uninterrupted contact center functionality, if you receive an email about upcoming certificate expiration dates, you must renew the security certificates before they expire.

Security Manager uses the Microsoft Windows Task Scheduler to schedule the weekly security store inspection. You must ensure that there is a Microsoft Windows user account that has the necessary privileges from which Security Manager can schedule a task on Windows Task Scheduler. You can use the Windows administrator account that you used to install Contact Center to add a task to Windows Task Scheduler.

Security Manager uses a specified Simple Mail Transport Protocol (SMTP) server to send the notification emails to the administrator's email address. Contact Center does not provide this SMTP server. You must provision this SMTP server and ensure that the Contact Center server can communicate with it at all times. Contact Center does not support Secure Sockets Layer (SSL) connectivity to this SMTP server.

Backing up the security store

About this task

Back up the security store for restoring the server or before creating a new security store. Keeping a backup of the security store allows you to restore Security Manager if there is a failure with the current store.

Important:

Record the password for this security store. If you restore this backup, you will need the security store password to log on to Security Manager.

Before you begin

- Read the security section of *Avaya Aura® Contact Center Overview and Specification*.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the security store password, and click **OK**.
4. On the Security Manager screen, select the **Store Maintenance** tab.
5. Under **Backup and Restore Security Store**, click **Browse**.
6. On the Select Directory dialog, browse to the folder where you want to back up the security store.

7. Click **Select Directory**.
8. On the Store Maintenance screen, click **Backup**.

   Security Manager displays the result of the backup and updates the **Last Backup** section.
9. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Deleting a security store

About this task

Delete an existing Contact Center security store when it is no longer required. You can delete an active or an offline security store.

Procedure

1. Use the System Control and Monitor Utility to stop all Contact Center services.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Security Manager screen, select the **Security Store** tab.
4. Click **Delete Store**.
5. On the Security Manager — Delete Store Confirmation dialog, click **Delete Store**.

   Security Manager deletes the store and updates the **Store Status** to “NOT CREATED”.
6. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Creating a new security store

About this task

The Security Manager uses a store to hold Certificate Authority root certificates and signed certificates. Create the security store if you plan to use a Certificate Authority and generate signed certificates.

The default encryption setting is SHA2 with a key size of 2048. For backward compatibility, you can choose SHA1 or a key size 1024. However, neither SHA1 nor 1024 provide the industry-recommended level of encryption. If you select one of these values, Contact Center displays a warning message.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.

3. In the **Security Manager** window, select the **Security Store** tab.
4. In the **Security Store** tab, in the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

   Important:

   The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.
5. In the **Name of Organizational unit** box, type the name of the department or division within the company.
6. In the **Name of Organization** box, type the company name.
7. In the **City or Locality** box, type the name of the city or district in which the contact center is located.
8. In the **State or Province** box, type the state or province in which the contact center is located.
9. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
10. In the **Security Store password** box, type a password for accessing the new security store.
11. In the **Confirm Store password** box, confirm the password for accessing the new security store.

    Important:

    Ensure you remember this password, because you will need it the next time you log on to Security Manager. If you forget the password, you will not be able to access Security Manager.
12. If you want to change the encryption setting, select the required encryption settings from the **Encryption Algorithm** and **Key Size** drop-down lists.

    The default value for **Encryption Algorithm** is SHA2 and the default value for **Key Size** is 2048.

    Contact Center displays a warning message if you select SHA1 or 1024. Contact Center includes these values for backward-compatibility only, because these settings do not meet the industry-recommended level of encryption.
13. Click **Create Store**.

    Contact Center creates the private key required for private-public key encryption.

    Security Manager automatically displays the Certificate Request tab, showing the newly created Certificate Signing Request file contents.

    Contact Center automatically backs up the new security store to the folder `D:\Avaya\Contact Center\autoBackUpCertStore`. Do not overwrite or delete this backup location.

14. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Next steps

Send the Certificate Signing Request file to the Certificate Authority, and receive a signed server certificate, so that you can import the server certificate to the security store.

Creating a security store with Subject Alternative Names

About this task

If you are implementing High Availability in the contact center, generate the security store using Subject Alternative Names (SANs). Include the Managed name and the current server name as SANs.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. In the **Security Manager** window, select the **Security Store** tab.
4. In the **Security Store** tab, in the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

   Important:

   The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.
5. In the **Name of Organizational unit** box, type the name of the department or division within the company.
6. In the **Name of Organization** box, type the company name.
7. In the **City or Locality** box, type the name of the city or district in which the contact center is located.
8. In the **State or Province** box, type the state or province in which the contact center is located.
9. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
10. Under **Subject Alternative Name (SAN)**, for each SAN you want to add:
    a. From the **Type** drop-down list, select DNS.
    b. In the **Value** field, type the FQDN for the server.
    c. Click **Add SAN**.

For a High Availability system, add the current server name and the Managed name for the HA pair.

11. On the Security Store tab, in the **Security Store password** box, type a password for accessing the new security store.
12. In the **Confirm Store password** box, confirm the password for accessing the new security store.

    Important:

    Ensure you remember this password, because you will need it the next time you log on to Security Manager. If you forget the password, you will not be able to access Security Manager.
13. If you want to change the encryption setting, select the required encryption settings from the **Encryption Algorithm** and **Key Size** drop-down lists.

    The default value for **Encryption Algorithm** is SHA2 and the default value for **Key Size** is 2048.

    Contact Center displays a warning message if you select SHA1 or 1024. Contact Center includes these values for backward-compatibility only, because these settings do not meet the industry-recommended level of encryption.
14. Click **Create Store**.

    Contact Center creates the private key required for private-public key encryption.

    Security Manager automatically displays the Certificate Request tab, showing the newly created Certificate Signing Request file contents.

    Contact Center automatically backs up the new security store to the folder `D:\Contact Center\autoBackUpCertStore`. Do not overwrite or delete this backup location.
15. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Next steps

Send the Certificate Signing Request file to the Certificate Authority, and receive a signed server certificate, so that you can import the server certificate to the security store.

Copying the Certificate Signing Request file

Before you begin

- Speak with your System Administrator to identify a Certificate Authority.

About this task

Security Manager automatically generates a Certificate Signing Request (CSR) when it creates a new security store. The Security Manager—Certificate Request tab displays the name, location,

and contents of the Certificate Signing Request (CSR) file on the server. A Certificate Authority uses this Certificate Signing Request (CSR) file to generate a signed security certificate. Contact Center uses the signed security certificate to establish secure communication links with Application Enablement Services (AES) servers, the Agent Browser application, and Web Services clients.

Until you add a signed certificate, the Signing Request Status field shows the CSR status as Pending. When the CSR is signed, and you add it to the security store using the “Add Certificate Tab”, the status changes to “Signed” to indicate that this CSR has been signed.

Procedure

1. Log on to the Contact Center server containing the security store.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. Select the **Certificate Request** tab.
4. Check the **Signing Request Status** value. If this value is **Pending**, you must have the CSR signed by a Certificate Authority.
5. Note the location of the Certificate Signing Request file from **File location**.
6. Select **Logout**.
7. Copy the Certificate Signing Request file from the directory referenced in **File location**, to send to a Certificate Authority.
8. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Next steps

After you perform this procedure, the certificate must be signed by a Certificate Authority. Contact your System Administrator for the preferred method of processing the signed certificate request file to obtain a signed certificate. Send the Certificate Signing Request file to a Certificate Authority and receive a signed certificate and root certificate to import to the security store.

Adding certificate files to the security store

Before you begin

- Use the CSR file from the Contact Center Security Manager to obtain a Certificate Authority signed server certificate and root certificate.
- Save the certificate files on the Contact Center server.

About this task

Contact Center Security Manager can add both Certificate Authority root certificates and signed server certificates to the security store. Contact Center requires a signed server certificate and a corresponding Certificate Authority root certificate to communicate using secure services.

There are two options when adding CA root and signed server certificates.

Automatically adding certificates :

You can select a folder that contains signed server and root certificates. Security Manager accesses this folder and automatically determines which are server certificates and which are root certificates and then adds them to the security store accordingly.

Important:

Security Manager attempts to import all files and certificates it finds in the certificate folder. Ensure that the certificate folder contains only CA root certificates and server certificates.

Manually adding certificates :

For manually added certificates, you can browse for individual signed server and root CA certificates and add them to the security store, one at a time. Security Manager checks the certificates and does not add server certificates as root CA certificates.

Procedure

1. Log on to the Contact Center server containing the security store.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the **Store Access** dialog, type the security store password.
4. Click **OK**.
5. In the Security Manager window, select the **Add Certificate** tab.
6. To add certificates automatically:
   a. Click **Browse**.
   b. On the Select Directory dialog, browse to the directory where you saved the certificate files, and click **Select Directory**.

      Security Manager displays the certificates in the **Certificates** field.
   c. Click **Add all Certificates**.
7. To add certificates manually:
   a. Select **Add Certificates Manually**.
   b. To manually add a CA root certificate, click **Browse**.
   c. Browse to the CA root certificate, and click **Select File**.
   d. Click **Add CA Certificate**.
   e. To manually add a server certificate, click **Browse**.
   f. Browse to the CA signed server certificate, and click **Select File**.
   g. Click **Add Signed Certificate**.
8. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Exporting a root certificate from the security store

About this task

Export the CA root certificate from the Contact Center security store so that clients using secured services can trust the public key for encryption. Avaya recommends that you always export the root certificate from the security store, so that it is consistent with the current server certificate.

Before you begin

- Add a server certificate and root certificate to the security store.

Procedure

1. Log on to the Contact Center server containing the store.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the **Store Access** dialog, type the security store password, and click **OK**.
4. In the Security Manager window, select the **Store Maintenance** tab.
5. In the **Root Certificates** field, select the root certificate that you want to export.
6. Click **Export**.
7. On the Select Directory To Export To dialog, select or create a directory to which you want to export the root certificate.
8. Click **Export To**.

   Security Manager exports two files to the directory. The PEM file is for AES only; the Security Certificate file is for all other clients.
9. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Next steps

Apply the root certificate to all Contact Center clients.

Applying the root certificate to a Contact Center client

About this task

Copy the root certificate exported from the Contact Center security store to the Contact Center clients and servers that use secure services. If you have a large number of clients, you can use automated methods to distribute and apply the root certificates. For example, you can use a Group Policy to distribute root certificates to clients using supported Microsoft Windows operating systems.

This procedure shows how to manually apply a root certificate on a Microsoft Windows operating system.

Before you begin

- Add a signed certificate and root certificate to the security store.
- Export the root certificate from the security store.

Procedure

1. On the client operating system Desktop, click **Start** > **Run**.
2. Type `MMC`, and click **OK**.
3. Click **File** > **Add/Remove Snap In**.
4. From the **Available snap ins** list, select **Certificates**, and click **Add**.
5. On the Certificates Snap in dialog, select **Computer account**, and click **Next**.
6. Click **Finish**.
7. On the Add or Remove Snap-ins dialog, click **OK**.
8. In the console root, expand **Certificates (Local Computer)** and then expand **Trusted Root Certification Authorities**.
9. Right-click the **Certificates** folder.
10. Select **All Tasks** > **Import**.
11. On the Certificate Import Wizard dialog, click **Next**.
12. Click **Browse**, and browse to the location where you copied the root certificate file.
13. Select the root certificate file and click **Open**.
14. On the Certificate Import Wizard dialog, click **Next**.
15. Click **Next**.
16. When the Certificate Import Wizard finishes importing the certificate, click **Finish**.

Creating an offline store

Before you begin

- Ensure that a security store already exists.

About this task

Create an offline security store if you want to replace the existing active security store, and minimize downtime. The procedure to create an offline store is the same as creating an active security store.

Security Manager uses a store to hold Certificate Authority root certificates and signed certificates. Create the security store if you plan to use a Certificate Authority and generate signed certificates.

The default encryption setting is SHA2 with a key size of 2048. For backward compatibility, you can choose SHA1 or a key size 1024. However, neither SHA1 nor 1024 provide the industry-

recommended level of encryption. If you select one of these values, Contact Center displays a warning message.

You cannot make any security configuration changes in Security Manager while you are viewing the offline store.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. In the **Security Manager** window, click **Store Commands** > **Create Offline Store**.
4. In the **Security Store** tab, in the **Full Computer Name (FQDN)** box, type the full FQDN of the server on which you are creating the security store.

   Important:

   The FQDN must be the full machine name of the server that the Security Store resides on. The FQDN name is case-sensitive.
5. In the **Name of Organizational unit** box, type the name of the department or division within the company.
6. In the **Name of Organization** box, type the company name.
7. In the **City or Locality** box, type the name of the city or district in which the contact center is located.
8. In the **State or Province** box, type the state or province in which the contact center is located.
9. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
10. In the **Security Store password** box, type a password for accessing the new security store.
11. In the **Confirm Store password** box, confirm the password for accessing the new security store.

    Important:

    Ensure you remember this password, because you will need it the next time you log on to Security Manager. If you forget the password, you will not be able to access Security Manager.
12. If you want to change the encryption setting, select the required encryption settings from the **Encryption Algorithm** and **Key Size** drop-down lists.

    The default value for **Encryption Algorithm** is SHA256 and the default value for **Key Size** is 2048.

    Contact Center displays a warning message if you select SHA1 or 1024. Contact Center includes these values for backward-compatibility only, because these settings do not meet the industry-recommended level of encryption.

13. Click **Create Store**.

    Contact Center creates the private key required for private-public key encryption.

    Security Manager automatically displays the Certificate Request tab, showing the newly created Certificate Signing Request file contents.

    Contact Center automatically backs up the new security store to the folder `D:\Avaya\Contact Center\OfflineAutoBackUpCertStore`. Do not overwrite or delete this backup location.

14. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Switching between the active and offline security stores

About this task

When an active and offline security store exist, you can view either store without any impact to Contact Center operation. Security Manager displays a message indicating which store you are currently viewing. You cannot make configuration changes to the offline security store.

Before you begin

- Ensure that an active and offline security store already exist.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. In the **Security Manager** window, click **Store Commands** > **View**.

   Depending on which store you are currently viewing, you can choose to view the other security store. Security Manager displays a message indicating which store you are currently viewing.

Making an offline store active

About this task

When the offline security store is ready to be placed into production, you can activate the offline store using Security Manager.

Note:

You must restart the Contact Center server after activating the offline store.

Before you begin

- Ensure that an active and offline security store already exist.
- Stop Contact Center services.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. In the **Security Manager** window, click **Store Commands** > **View** > **Offline Store**.
4. In the **Security Manager** window, click the **Make Active** button.
5. Click **Confirm** to apply the new security settings and activate the offline store.

   A message appears under **Store Status** to indicate that the Make Active operation was successful. The offline security store is now the new active security store. The old active security store is now the offline store.
6. Restart the Contact Center server.

Next steps

After restarting the Contact Center server, verify the configuration settings for the new active security store using the **Security Configuration** tab in Security Manager.

Turning on Web Services security

About this task

Turn on Web Services security if you want to use HTTPS security for management and agent operations.

Before you begin

- Read the security section of *Avaya Aura® Contact Center Overview and Specification*.
- Create a new security store and import the signed server certificate and root certificate from the CA.
- Export the CA root certificate from the security store, and apply it to all the CCMA and Agent Desktop clients in the contact center.

Procedure

1. Log on to the server as a local administrator.

   Important:

   If you log on to the server as a domain administrator, this procedure does not complete successfully.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.

3. On the Store Access dialog, type the password for the security store, and click **OK**.
4. On the Security Manager screen, select the **Security Configuration** tab.
5. Click **Security On**.
6. Click **Apply**.
7. On the Security Change Confirmation dialog, click **Confirm**.
8. Click **Log Out**.
9. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Configuring the minimum TLS version

About this task

Configure minimum TLS versions that Contact Center can negotiate for secure connections. This enables third-party and legacy systems that do not support TLS 1.2 to communicate securely with Contact Center. If you do not change these settings, Contact Center uses only TLS 1.2, and does not connect to systems that support only lower versions of TLS.

You can set minimum TLS versions separately for the following communications:

- SIP and CTI signaling
- CCMA and CCMM administration
- Event Broker Web service (this setting also sets the minimum TLS version used for Web Statistics)

Before you begin

- Read the security section of *Avaya Aura® Contact Center Overview and Specification*.
- Create a new security store and import the signed server certificate and root certificate from the CA.
- Export the CA root certificate from the security store, and apply it to all the CCMA and Agent Desktop clients in the contact center.

Procedure

1. Log on to the server as a local administrator.

   Important:

   If you log on to the server as a domain administrator, this procedure does not complete successfully.

2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the password for the security store, and click **OK**.
4. On the Security Manager screen, select the **Security Configuration** tab.

5. In the **SIP and CTI Signalling Level** box, select the lowest version of TLS for SIP and CTI signaling communication.
6. In the **CCMA — Multimedia Web Service Level** box, select the lowest version of TLS for CCMA and Multimedia Web service communication.

   This changes the setting for IIS, and for Windows Server 2012 generally.
7. In the **Event Broker Web Service Level** box, select the lowest version of TLS for Event Broker Web Service communication.
8. Click **Apply**.
9. Click **Log Out**.
10. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Configuring SMTP server details

Before you begin

- Provision, configure, and maintain a Simple Mail Transport Protocol (SMTP) server. Contact Center Security Manager supports Microsoft Exchange Server.
- Know the authentication logon account and password details for the SMTP server.
- Ensure that the Contact Center server can access the SMTP server at all times.
- On the SMTP server, configure an email address for the contact center administrator. Security Manager sends the notification emails to this address. Ensure the contact center administrator monitors this email address.
- On the SMTP server, configure an email address for Avaya Aura® Contact Center Security Manager. Security Manager can then use this email address to send notification emails.

About this task

Configure the details of the SMTP server and accounts used to send the Security Manager status report email.

Procedure

1. On the **Security Manager** screen, select the **Expiration Alerts** tab.
2. Select **SMTP Configuration**.
3. From the **Outgoing e-mail server (SMTP)** list, select **IP** or **Address**. The Contact Center server must be able to communicate with the SMTP server by IP address or SMTP address.
4. In the **Outgoing e-mail server (SMTP)** box, enter the IP address or SMTP address of the SMTP server.
5. In the **Port number** box, enter the TCP port number for the SMTP server. The default port number is 25.

6. In the **Sender e-mail address** box, enter the email address to be used by Security Manager to send notification emails. Ensure this email address is registered with the SMTP server.
7. In the **Recipient e-mail address** box, enter the email address to which Security Manager is to send the notification emails. Ensure this email address is registered with the SMTP server. This is typically the contact center administrator's email address. You must monitor this email address for notifications about the status of Contact Center security certificates.
8. If your SMTP server requires authentication, select **SMTP server requires authentication**. If your SMTP server does not require authentication, clear this check box.
9. In the **User name** box, enter the user account name used to authenticate with the SMTP server.
10. In the **Password** box, enter the password of the user account used to authenticate with the SMTP server.
11. Click **Save Configuration**.
12. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Scheduling a security store inspection task

Before you begin

- Configure the SMTP server and email account details.

About this task

Schedule a security store inspection task. Security Manager adds the scheduled task to the underlying Windows Task Scheduler. The scheduled task runs the security store inspection utility once a week. You can select the time and day of the week that the security store inspection task runs during the week.

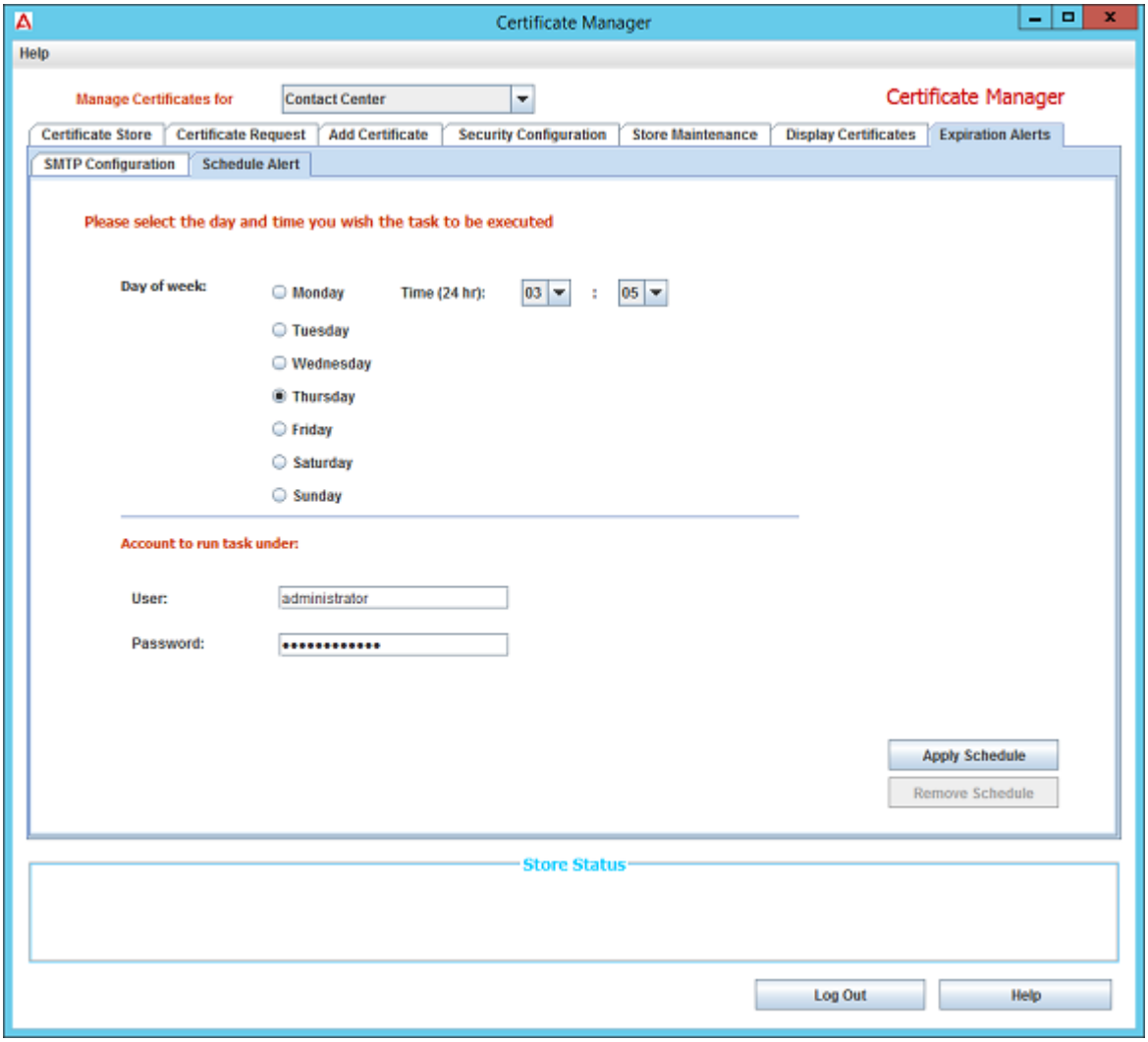
Procedure

1. Log on to the Avaya Aura® Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. Select **Expiration Alerts** > **Schedule Alerts**.
4. To enable the weekly inspection task, select **Schedule alerts**.
5. From the **Day of week** list, select the day on which to schedule the weekly inspection task.
6. In the **Time (24 hr)** section, enter the time of day on which to schedule the weekly inspection task. Use twenty four hour format time.
7. In the **User** box, enter the name of a Windows user account that has the privileges necessary to access the Windows Task scheduler and schedule the task.

8. In the **Password** box, enter the password of the Windows user account that has the privileges necessary to access the Windows Task scheduler and schedule the task.
9. Click **Apply Schedule**.

   Security Manager then schedules this task on the underlying Microsoft Windows Task Scheduler. After successfully scheduling the task, the name on the **Apply Schedule** button changes to **Modify Schedule** and the button is disabled. To enable the **Modify Schedule** button, select a new time. You can then update the scheduled task time by clicking **Modify Schedule**.

   Example of a scheduled task:



10. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Verifying the scheduled security store inspection task

Before you begin

- Configure the scheduled task.

About this task

Verify that the Windows Task Scheduler lists the Security Manager scheduled inspection task. Do not modify the scheduled task in Task Scheduler. Use only Security Manager to modify the scheduled inspection task.

Procedure

1. Log on to the Contact Center server.
2. On the **Start** screen, under **Administrative Tools**, click **Task Scheduler**.
3. In the left pane, click **Task Scheduler Library**.
4. In the middle pane, confirm that there is a task named **aaccSentinel**.
5. Confirm that the task **Status** is **Ready**.
6. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Examining a certificate file in the security store

Before you begin

- The security store must contain one or more certificate.

About this task

View the certificates in the store using the Security Manager Display Certificates tab.

Procedure

1. Log on to the server containing the store.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. In **Store Access**, enter the security store password.
4. Click **OK**.
5. Select the **Display Certificates** tab.
6. Select **List**, to list all stored certificates in the store.
7. Select a certificate.

   The details of the certificate are displayed.
8. Select **Close**.

Removing a certificate file from the security store

Before you begin

- Save the certificate files on your security store computer.

About this task

You can remove the certificates added to the store manager by using the Store Maintenance tab of the Security Manager.

Procedure

1. Log on to the server containing the store.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. In **Store Access**, type the security store password.
4. Click **OK**.
5. In the **Security Manager** window, Select the **Store Maintenance** tab.
6. Under **Signed and Root Certificates that reside in the store**, Security Manager lists all certificates in the store.
7. To delete a signed certificate, click **Delete Signed Cert** and click **OK**.
8. To delete a root certificate, select the certificate to remove from the **Root Certificates** list and click **Delete**.

Modifying a scheduled security store inspection task

Before you begin

- Configure the scheduled task.

About this task

Modify the time of day for an existing scheduled task. For an existing scheduled task, you can change only the time of day; you cannot change the day of week for an existing scheduled task.

This is an optional procedure.

Procedure

1. Log on to the Avaya Aura® Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. In **Store Access**, type the certificate store password.
4. Click **OK**.
5. Select **Expiration Alerts** > **Schedule Alert**.

6. In the **Time (24 hr)** section, enter the new time of the day on which to schedule the security store inspection task. Use twenty four hour format time.
7. In the **User** box, enter the name of a Windows user account that has the privileges necessary to access the Windows Task scheduler and schedule a task.
8. In the **Password** box, enter the password of the Windows user account that has the privileges necessary to access the Windows Task scheduler and schedule the task.
9. Click **Modify Schedule**.

   Security Manager then schedules this task to run at the new time of day on the underlying Microsoft Windows Task Scheduler.

Removing a scheduled security store inspection task

Before you begin

- Configure the scheduled task.

About this task

Remove the Security Manager activated scheduled task from the Windows Task Scheduler. If you delete the scheduled security store inspection task, Security Manager no longer sends notification emails when Security Manager security certificates are due to expire. You must then manually monitor the status and expiration dates of the security certificates.

Procedure

1. Log on to the Avaya Aura® Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. In **Store Access**, type the certificate store password.
4. Click **OK**.
5. Select **Expiration Alerts** > **Schedule Alerts**.
6. Click **Remove Schedule**.

Recreating the CCMA security bindings

About this task

When you delete the security store, Contact Center removes the CCMA security bindings to IIS. To recreate these bindings, you must turn on Web Services security, apply the setting, and turn off web services security.

Before you begin

- Add certificate files to the security store.

Procedure

1. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
2. On the Store Access dialog, type the password for the security store, and click **OK**.
3. On the Security Manager screen, select the **Security Configuration** tab.
4. Click **Security On**.
5. Click **Apply**.
6. On the Security Change Confirmation dialog, click **Confirm**.
7. Click **Security Off**.
8. Click **Apply**.
9. On the Security Change Confirmation dialog, click **Confirm**.
10. Click **Log Out**.
11. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

    For the Multimedia Contact Server, you must reboot the server to complete the procedure.

Turning off Web Services security

About this task

Turn off Web Services security if you want to stop using the feature.

Before you begin

- Read the security section of *Avaya Aura® Contact Center Overview and Specification*.

Procedure

1. Log on to the server as a local administrator.

   Important:

   If you log on to the server as a domain administrator, this procedure does not complete successfully.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the password for the default security store, and click **OK**.
4. On the Security Manager screen, select the **Security Configuration** tab.
5. Click **Security Off**.

6. Click **Apply**.
7. On the Security Change Confirmation dialog, click **Confirm**.
8. Click **Log Out**.
9. If you have a Multimedia Contact Server, repeat this procedure on the Multimedia Contact Server.

Next steps

Instruct all users in the contact center to use `http` instead of `https` when connecting to the server from CCMA clients or Agent Desktop.

Chapter 39: Database encryption administration

This chapter describes the steps you need to perform to encrypt the Contact Center database. Using Security Manager, you can create and activate an encryption key and use it to encode the files in the Contact Center Caché database.

Caution:

You must back up the encryption key, and the encryption key credentials. If you lose the encryption key or its credentials, they are not retrievable. This can result in loss of service.

You can also use Security Manager to decrypt the Contact Center database.

Important:

You must perform Contact Center database encryption or decryption during a scheduled maintenance window.

High Availability

In a High Availability (HA) solution, you must use the same encryption key on all Contact Center servers in the solution. Contact Center supports HA solutions where the Active server database is encrypted and the Standby server database is not encrypted, and vice versa. Database shadowing remains operational regardless of the encryption status of the Contact Center database. This allows you to minimize downtime while you implement database encryption in your solution. If you want to encrypt the databases in a HA solution, you can use the following procedure to minimize downtime:

1. Stop all Contact Center services on the standby server system (Server B).
2. Encrypt the standby server database (Server B).
3. Start the standby server B. Ensure that you synchronize the data between the servers.
4. Run a manual switchover, the current standby Server B becomes an active server. Server B is now running and processing contacts.
5. Stop all Contact Center services on Server A.
6. Encrypt the new standby server database (Server A). You must use the same encryption key as you used to encrypt Server B.
7. Backup all the contact center databases on the active server, Server B.
8. Restore all the active Server B contact center database backups onto Server A.
9. Configure High Availability on the standby Server A.
10. Configure standby Server A for your contact center.

11. Start the standby Server A. Ensure that data is synchronized between the servers.
12. Run a manual switchover if required, the current standby Server A becomes an active server. Server A is now running and processing contacts.

Upgrades

Before you upgrade your Contact Center solution, you must ensure that all databases are not encrypted.

Creating and activating an encryption key

About this task

Create and activate an encryption key and use it to encode the files in the Contact Center Caché database.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the security store password, and click **OK**.
4. On the Security Manager screen, select the **Database Encryption** tab.
5. Under **Credentials**, in the **User Name** box, type the user name for the new encryption key.
6. In the **Password** box, type the password for the new encryption key.

   Note:

   Passwords must be between 8 and 20 characters in length, and include at least one number, at least one uppercase letter, at least one lowercase letter, and no spaces. Passwords must not contain any of the following characters: **& " : > |**.
7. Under **Create/Select and Activate Key**, click **Browse**.
8. Browse to the folder where you want to save the encryption key.
9. In the **File Name** box, type a name for the key and click **Save File**.
10. Click **Create and/or Activate Key**.
11. On the **Confirm Password** dialog box, type the encryption key password and click **OK**.

    The **Output** pane shows the progress of the task.

Next steps

Caution:

You must back up the encryption key, and the encryption key credentials. If you lose the encryption key or its credentials, they are not retrievable. This can result in loss of service.

Encrypting the Contact Center database

About this task

Encrypt the Contact Center database during a scheduled maintenance window to ensure that sensitive data is secure.

Before you begin

- Create an encryption key, and ensure that the location of the key is accessible from the Contact Center server.
- Stop Contact Center services.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the security store password, and click **OK**.
4. On the Security Manager screen, select the **Database Encryption** tab.
5. Under **Credentials**, in the **User Name** box, type the user name for the encryption key.
6. In the **Password** box, type the password for the encryption key.

   Note:

   Passwords must be between 8 and 20 characters in length, and include at least one number, at least one uppercase letter, at least one lowercase letter, and no spaces. Passwords must not contain any of the following characters: **& " : > |**.
7. Under **Encrypt/Decrypt Database**, if the **Key Location** box is not already populated with the encryption key location, click **Browse**.
8. In the **Select Key File** window, navigate to the location of the encryption key.
9. Select the encryption key file and click **Select File**.
10. Click **Encrypt**.

    The **Output** pane shows the progress of the task. The amount of time this task takes depends on the size of the Contact Center database.

Next steps

When the encryption is complete, start Contact Center services.

Decrypting the Contact Center database

About this task

Decrypt the Contact Center database during a scheduled maintenance window. Before you upgrade Contact Center software, you must decrypt the database.

Before you begin

- Ensure that the location of the encryption key is accessible from the Contact Center server.
- Stop Contact Center services.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the security store password, and click **OK**.
4. On the Security Manager screen, select the **Database Encryption** tab.
5. Under **Credentials**, in the **User Name** box, type the user name for the encryption key.
6. In the **Password** box, type the password for the encryption key.
7. Under **Encrypt/Decrypt Database**, click **Browse**.
8. In the **Select Key File** window, navigate to the location of the encryption key.
9. Select the encryption key file and click **Select File**.
10. Click **Decrypt**.

    The **Output** pane shows the progress of the task. The amount of time this task takes depends on the size of the Contact Center database.

Next steps

When the decryption is complete, start Contact Center services.

Chapter 40: Windows Server 2012 security for Contact Center

Contact Center installs and updates sometimes modify Group Policies and account settings on the Windows Server 2012 operation system. The topics in this chapter outline how to change or maintain the default configuration that Contact Center applies.

Disabling Server Message Block signing in the server local group policy

About this task

Both the Contact Center DVD and the Release Pack installer modify the Windows Server 2012 local group policy to enable Server Message Block (SMB) signing. SMB signing places a digital “tag” into each server message block, which helps prevent man-in-the-middle attacks on network file sharing.

If you do not want to use SMB signing, follow this procedure to disable it by modifying the Windows Server 2012 local group policy.

Procedure

1. Log on to the Contact Center server as Administrator.
2. On the **Desktop** screen, right-click **Start** and select **Run**.
3. In the **Run** text box, type `gpedit.msc`.
4. Click **OK**.
5. On the Local Group Policy Editor window, in the left pane, select **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.
6. In the Name column, right-click **Microsoft network client: Digitally sign communications (always)**, and select **Properties**.
7. On the Microsoft network client: Digitally sign communications (always) dialog, select **Disable**.
8. In the Name column, right-click **Microsoft network server: Digitally sign communications (always)**, and select **Properties**.

9. On the Microsoft network server: Digitally sign communications (always) dialog, select **Disable**.

Chapter 41: Avaya Aura® Media Server security certificates administration

Contact Center and Avaya Aura® MS include a number of services and connections that you can secure using Transport Layer Security (TLS). If you enable Web Services security on Contact Center, then you must copy the Contact Center root certificate to Avaya Aura® MS.

The Avaya Aura® MS security store can include multiple server certificates and root certificates. Avaya Aura® MS supports assigning different certificates to different Avaya Aura® MS services.

High Availability

In a High Availability (HA) system, the server certificate must use Subject Alternative Names (SANs). Include a SAN for the Avaya Aura® MS Managed IP address and the server IP address. This ensures clients connecting to Avaya Aura® MS using the managed IP address do not get warnings that the signed certificate name does not match the server name.

Importing the Contact Center root certificate into Avaya Aura® MS

Before you begin

- Export the root certificate from the Contact Center Security Store, and save the PEM file to a location on the Avaya Aura® MS server.

About this task

Import the Contact Center root certificate into the Avaya Aura® MS trust store to support Transport Layer Security (TLS) communications. You perform this procedure on the Avaya Aura® MS server. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server. Avaya Aura® MS supports importing only the PEM format root certificate file.

Procedure

1. Log on to Avaya Aura® MS Element Manager.
2. Navigate to **EM** > **Security** > **Certificate Management** > **Trust Store**.
3. Click **Import**.

4. In the **Trust friendly name** field, type a friendly name for the CA root certificate.
5. Click **Browse**.
6. Select the root certificate file that you exported from the Contact Center Security Store.
7. Click **Save**.
8. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server.

Creating a new certificate signing request for Avaya Aura® Media Server

About this task

Create a Certificate Signing Request (CSR) file to send to a Certificate Authority (CA) to get a signed server certificate. You use the signed server certificate to secure services provided by Avaya Aura® MS. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server.

Procedure

1. Log on to Avaya Aura® MS Element Manager.
2. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
3. In the **Key Certificates** section, click **Create New**.
4. On the Create New Certificate screen, in the **Signing authority** field, select **Other Certificate Authorities**.
5. In the **Certificate friendly name** field, type a name for this certificate.
6. In the **Key bit length** field, select **2048**.
7. In the **Signature algorithm** field, select **SHA-2/SHA-512**.
8. In the **Organization** field, type the company name.
9. In the **Organization unit** field, type the name of the department or division within the company.
10. In the **Common name** field, type the FQDN of the Avaya Aura® MS server.
11. In the **Country (ISO 3166)** box, type the country code in which the contact center is located.
12. In the **State / Province (full name)** box, type the state or province in which the contact center is located.
13. In the **City / Locality** box, type the name of the city or district in which the contact center is located.
14. If this Avaya Aura® MS server is part of a HA pair, select **Include Subject Alternative Name with FQDN**, and type the full FQDN for the managed name of the HA pair.

15. Click **Save**.
16. Select the location where you want to save the CSR file.
17. Click **Save**.

    Avaya Aura® MS displays the Key Store screen, with the new certificate listed in a Pending state.
18. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server.

Next steps

After you perform this procedure, the certificate must be signed by a Certificate Authority. Contact your System Administrator for the preferred method of processing the CSR file to obtain a signed certificate. Send the CSR file to a Certificate Authority and receive a signed server certificate and root certificate to import to the Avaya Aura® MS key store.

Adding signed certificate files to the Avaya Aura® MS key store

About this task

Add the Certificate Authority (CA) root certificate and signed server certificate to the Avaya Aura® MS key store. Avaya Aura® MS requires a signed server certificate and a corresponding Certificate Authority root certificate to communicate using secure services.

Before you begin

- Use the CSR file that you created to obtain a CA signed server certificate and root certificate.
- Save the certificate files on the Contact Center server.

Procedure

1. Log on to Avaya Aura® MS Element Manager.
2. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
3. In the **Key Certificates** section, select the Pending certificate.
4. Click **Process Certificate Signing Request**.
5. On the Process Certificate Signing Request screen, click **Browse**.
6. On the Choose File to Upload dialog, browse to the location where you downloaded the certificate file from the CA, and select the file.
7. Click **Open**.
8. On the Process Certificate Signing Request screen, click **Process Signed Certificate**.
9. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server.

Next steps

Specify the Avaya Aura® MS services that use the new server certificate, and export the CA root certificate to the clients that use those services.

Assigning a server certificate to an Avaya Aura® MS service profile

About this task

Assign a server certificate to one or more Avaya Aura® MS services, to use that server certificate to secure those services.

Before you begin

- Add a signed server certificate and corresponding root certificate to the Avaya Aura® MS key store.

Procedure

1. Log on to Avaya Aura® MS Element Manager.
2. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
3. On the Process Certificate Signing Request screen, in the **Service Profiles** section, click **Assign**.
4. On the Assign Certificate screen, select the new certificate for each service profile that you want to secure.
5. Click **Save**.
6. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server.

Next steps

Export the CA root certificate from Avaya Aura® MS, and import it to the clients that use the secured services.

Exporting a root certificate from Avaya Aura® MS in PKCS12 format

About this task

Export the CA root certificate from the Avaya Aura® MS server to import to clients that use the secured Avaya Aura® MS services, and can import PKCS12 format certificates.

Before you begin

- Add a signed server certificate and root certificate to the Avaya Aura® MS key store

Procedure

1. Log on to Avaya Aura® MS Element Manager.
2. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
3. In the **Key Certificates** section, select the server certificate for which you want to export the CA root certificate.
4. Click **Export**.
5. In the **Type** field, select **Export with Key**.
6. In the **Password for certificate export** field, enter a key.
7. Click **Export**.
8. On the File Save dialog, select a location for the file and save the file.
9. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server.

Next steps

Import the root certificate to clients that use the secured Avaya Aura® MS services.

Exporting a root certificate from Avaya Aura® MS in PEM format

About this task

Export the CA root certificate from the Avaya Aura® MS server to import to clients that use the secured Avaya Aura® MS services, and can import only PEM format certificates.

Before you begin

- Add a signed server certificate and root certificate to the Avaya Aura® MS key store

Procedure

1. Log on to Avaya Aura® MS Element Manager.
2. Navigate to **EM** > **Security** > **Certificate Management** > **Key Store**.
3. On the Process Certificate Signing Request screen, in the **Key Certificates** section, select the server certificate for which you want to export the CA root certificate.
4. Click **Export**.
5. In the **Type** field, select **Export in PEM Format**.
6. Click **Export**.
7. On the File Save dialog, select a location for the file and save the file.
8. If you have multiple Avaya Aura® MS servers, repeat this procedure on each server.

Next steps

Import the root certificate to clients that use the secured Avaya Aura® MS services.

Part 10: Common server administration

- Microsoft Windows configuration and management on page 483
- Simple Network Management Protocol administration on page 486
- Contact Center server High Availability on page 491
- Common procedures on page 519

Chapter 42: Microsoft Windows configuration and management

Perform the following procedures to configure settings for Microsoft Windows on your server.

Managing date and time features

About this task

Manage the date and time features in Microsoft Windows to avoid potential call processing outages.

Important:

You must not change the date backwards. You can change the date and time forwards.

Procedure

1. Log on to the server as Administrator.
2. On the **Start** screen, click **Control Panel**.
3. Click **Clock, Language, and Region**.
4. Click **Date and Time**.
5. In the **Date and Time** dialog box, click **Change time zone**.
6. Clear the **Automatically adjust clock for Daylight Saving Time** check box.
7. Click **OK**.
8. Click **OK** to save your changes.

Disabling the Windows time service

Before you begin

- Disable Date and Time features.

About this task

Disable the Windows Time service to stop it from running and attempting to synchronize the CCMS server time with a time source and to avoid potential call processing outages.

If the Contact Center Manager Server is in a SIP environment or is the Network Control Center server, you must skip this step.

Procedure

1. On the **Start** screen, click **Administrative Tools** > **Services**.
2. In the Services window, in the right pane, double-click **Windows Time**.
3. In the **Windows Time Properties** dialog box, on the **General** tab, in the **Service Status** area, click **Stop**.
4. From the **Startup** type list, select **Disabled**.
5. Click **Apply** to save your changes.
6. Click **OK** to close the **Windows Time Properties** dialog box.
7. Close the Services window.

Verifying Service Packs

Before you begin

- Look up the most recent patches and upgrades for your Contact Center Server at www.avaya.com.
- Review *Upgrading and patching Avaya Aura® Contact Center* to understand how to install Service Packs.

About this task

Verify that you have the most recent Service Packs for the Contact Center Manager Server software.

Procedure

1. Log on to the server on which you installed Contact Center Manager Server.
2. On the **Apps** screen, in the **Avaya** section, select **Update Manager**.
3. Click the **CCMS** tab.
4. View the most recent **Update Name**.
5. Compare the most recent update name in the Update Manager with the most recent patch or upgrade listed on the Avaya website.
6. Click **Close**.
7. Install missing Service Packs from the website by performing instructions present in *Upgrading and patching Avaya Aura® Contact Center*.

Configuring the operating system for remote access

Before you begin

- Add your server to a workgroup.

About this task

Configure remote access for your server in a workgroup to allow technical support to access the server.

Procedure

1. On the **Start** screen, click **Control Panel** > **System and Security**.
2. In the **System** section, click **Allow remote access**.
3. Click the **Remote** tab.
4. Select **Allow connections from computers running any version of Remote Desktop**.
5. Click **OK**.

Chapter 43: Simple Network Management Protocol administration

Windows provides a Simple Network Management Protocol (SNMP) agent, which runs as a service on each Contact Center server. Contact Center servers use this service to forward events to a Network Management System (NMS) on your network.

For more information about event codes and a list of recommended events to forward, see *Contact Center Event Codes*.

This chapter describes how to configure the Simple Network Management Protocol for your contact center.

Configuring Windows SNMP Service

About this task

Configure Windows Simple Network Management Protocol (SNMP) service on each Contact Center server to forward events to a Network Management System (NMS) on your network.

Procedure

1. Log on to the Contact Center server as Administrator.
2. On the **Start** screen, click **Administrative Tools** > **Services**.
3. In the Services window, select the **SNMP Service**.
4. Click **Action** > **Properties**.
5. In the SNMP Service Properties window, click the **Traps** tab.
6. If no community name is defined, in the **Community name** box, type `public`.
7. Click **Add to list**.
8. Click **Add** to add the IP address of the NMS to which the server sends traps.
9. In the SNMP Service Configuration window, type the IP address of the NMS.
10. Click **Add**.
11. In the SNMP Service Properties window, click **Add**.
12. In the Services window, right-click the **SNMP Trap** Service, and select **Start**.

13. Close the Services window.

Selecting CCMS events to be forwarded

About this task

Contact Center Manager Server uses SNMPFilterCnfg.exe to forward all Contact Center Manager Server related events (these events fall between the range 44900 to 51400).

Procedure

1. Using Windows Explorer, browse to the folder **D:\Avaya\Contact Center\Manager Server \bin**, and double-click **SNMPFilterCnfg.exe**.
2. In the **Level of Filtering** box, select the types of events that you want to forward to the Network Management System (NMS).

   Important:

   All event types that appear and the type that you select are also forwarded. For example, if you select Major, then all Unknown, Critical, and Major events are forwarded.
3. Click **OK**.

Selecting CCMA, LM, CCT, and CCMM events to be forwarded

About this task

Contact Center Manager Administration, License Manager, Communication Control Toolkit, and Contact Center Multimedia use the Windows Server 2012 R2 Event to Trap Translator (evntwin.exe) to select the events to be forwarded to the Network Management System (NMS).

When you are selecting events to forward, not all event sources populate the event descriptions. For some event sources the Event to Trap Translator shows event codes and descriptions, and for others it shows event codes.

Avaya provides a SNMP Trap Configuration File (.cnf) that is aligned with the *Contact Center Event Codes* document. Download the Contact Center Release 7.0 SNMP Trap Configuration File from the Avaya Support website at http://support.avaya.com. The file is available in the Contact Center software download Service Pack section. You can load this SNMP Trap Configuration file into the Event to Trap Translator on the Contact Center server.

In addition to the recommended SNMP Traps, you can add additional event codes to be forwarded to the NMS.

For more information about event codes, event source names, and a list of recommended events to forward, see *Contact Center Event Codes*.

Procedure

1. Download the Contact Center Release 7.0 SNMP Trap Configuration file (.cnf) from the Avaya Support website at http://support.avaya.com. The file is available in the Contact Center software download Service Pack section. Copy the .cnf file to the Contact Center server.
2. On the Contact Center server, open a command window and navigate to the location of the downloaded .cnf file.
3. Use the Windows `evntcmd` utility to load the SNMP Trap Configuration file.

   ```
   evntcmd -v 10 <SNMP Trap Configuration file name.cnf>
   ```

   For example:

   ```
   evntcmd -v 10 ACC_7_0_0_0_SNMP_Trap_File_ver1_0.cnf
   ```
4. On the **Desktop** screen, right-click the Windows icon and select **Run**.
5. In the **Run** text box, type `C:\Windows\System32\evntwin.exe`.
6. On the **Event to Trap Translator**, under **Configuration type**, select **Custom**.

   Ensure the recommended event traps from the *Contact Center Event Codes* document are listed.

   Important:

   Contact Center and related event sources are listed under several categories, including Application and System. License Manager events are listed under the NGEN event source.
7. Click **OK** to save the settings.
8. You can add additional event codes to be forwarded to the NMS.
   a. Click **Edit**.
   b. Under Event sources, click the folder for the event source you require.

      Important:

      Contact Center and related event sources are listed under several categories, including Application and System. License Manager events are listed under the NGEN event source.

   c. From the list of events, double-click the event you want to convert to an SNMP trap.
   d. On the **Properties** window, click **OK** if no change is required to generate the trap.
   e. Repeat these sub-steps for each event that you want added to the list of events to be translated into SNMP traps.
9. Close the Event to Trap Translator window.

Copying Event to Trap Translator settings from one Contact Center server to another

Before you begin

On Windows Server 2012 R2, use the Event to Trap Translator (evntwin.exe) to select the events to be forwarded to the Network Management System. For more information, see Selecting CCMA, LM, CCT, and CCMM events to be forwarded on page 487.

About this task

Copy Event to Trap Translator settings from one Contact Center server to another, for example from an active server to a standby server. The following procedure is an example of copying evntwin.exe settings from an active server to a standby server.

Procedure

1. Configure Event to Trap Translator settings on the active server.
2. On the active server, open the **Event to Trap Translator** window. On the **Desktop** screen, click **Start** > **Run**.
3. In the **Run** text box, type `C:\Windows\System32\evntwin.exe`
4. On the **Event to Trap Translator** window, select all of the event traps to copy and click **Export**.
5. On the **Export Events** dialog box select a location on the active server, type a name for the exported .cnf file, and click **Save**.
6. Copy the .cnf file from the active server to a location on the standby server.
7. On the standby server, open a command window and navigate to the location of the exported .cnf file.
8. Run the following command: `evntcmd -v 10 <Exported file name.cnf>`.
9. On the standby server, on the **Desktop** screen, click **Start** > **Run**.
10. In the **Run** text box, type `C:\Windows\System32\evntwin.exe`
11. Under **Configuration** type, ensure **Custom** is selected.
12. Ensure all of the event traps from the active server are listed.
13. Click **OK** to save the settings and close the **Event to Trap Translator** window.

Configuring the NMS

About this task

After you configure the server, you must configure the Network Management System (NMS) to receive and interpret traps (including identification to the NMS, and the origin and format of the Contact Center traps).

Load or compile the Contact Center Manager Server Management Information Block (MIB) files in the NMS. The following Contact Center Manager Server MIB files describe the format of the traps generated by Contact Center Manager Server:

- NB-FLT.mib - This is an SMNP v1 MIB that supports RFCs 1115,1212,1213 & 1215. This MIB describes the format of the traps that are sent from Contact Center Manager Server.
- RR-AACCDB.mib - This is an SNMP v2 MIB that supports RFCs 2578, 2579, & 2580. This MIB describes the format of the traps that are sent from the Contact Center Cache Database component.

You can use these files on the NMS system.

- The NB-FLT.mib file is available on the Contact Center Manager Server server, in the `D:\Avaya\Contact Center\Manager Server\data` folder.
- The RR-AACCDB.mib file is available on the Contact Center Manager Server server, in the `D:\Avaya\Contact Center\Common Components\Cache` folder.

Procedure

For more information about configuring your NMS, see your NMS documentation.

Chapter 44: Contact Center server High Availability

Avaya Aura® Contact Center supports campus High Availability for fault tolerant and mission critical contact centers. Contact Center supports the following levels of campus high availability:

- Mission Critical High Availability
- Hot standby High Availability

High Availability is a licensed feature. It is enabled when a standby server license is purchased.

Important:

CCT SOA configuration (CCT Web services) information is not replicated to standby or Remote Geographic Node (RGN) servers. Configure CCT Web services identically for the active CCT, the standby CCT, and the RGN server.

Mission Critical High Availability:

Use the High Availability Utility to configure Mission Critical High Availability IP addresses and to configure which server is the active server and which is the standby server. Then use the System Management and Monitoring Component (SMMC) system tray to enable and start Mission Critical High Availability functionality.

If a critical service is restarted on the active server, a switchover is not possible. The High Availability system stops functioning. To restart, use the System Management and Monitoring Component (SMMC) system tray and select Re-enable HA System.

Note:

In the SMMC system tray, the available menu options depend on the state of the HA System. For example, the Start HA menu option is available only when the High Availability system is in a stopped state. The state of the critical CCT and CCMS services affects the available SMMC system tray menu options. The state of the License Manager, Avaya Aura® Media Server, CCMA, and CCMM services does not affect the available SMMC system tray menu options.

Hot standby High Availability High Availability:

Hot-standby High Availability (HA) is configured using the High Availability Utility.

Geographic High Availability considerations:

Following a campus HA switchover, Avaya recommends that you take a backup of the new active server database and restore it on the RGN server. This ensures that the databases are correctly synchronized.

Prerequisites to Contact Center Server High Availability

Procedure

Install the standby server with the same configuration of drive letters and software, site name as the corresponding active server. See *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications* or *Avaya Aura® Contact Center Commissioning for Avaya Communication Server 1000*.

Configuring hot-standby managed IP address

About this task

A Managed IP address is a virtual IP address that is attached to a network adapter on the active server. Each Contact Center application server is assigned a static IP address. Once the active server in each replication pair has been determined, the active server attaches a Managed IP address to its network interface. The Managed IP address is assigned to the active server and it is used by all other Contact Center (CC) applications and clients to connect to that application. The standby server assumes this same managed IP address if it takes over processing and becomes the active application. The active server stops using the Managed IP when it stops being the active server.

Procedure

1. Log on to the server.
2. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
3. In the left pane of the High Availability window, expand **Configuration**.
4. Click **Server Mode**.
5. Under **Server Mode Configuration**, select **Standby**.
6. Confirm the IP addresses for the **Managed IP**, **Active Server details**, the **Standby Server details** and the **Trusted IP**.
7. Click **Save**.

Variable definitions

Name	Description
Server Mode Configuration	The mode of the server: • Active: The server that currently handles contacts. • Standby: The server that backs up operations if the active server fails.
Switchover	The length of time configured for server inactivity before the change to the Standby server for handling contacts.
Managed IP	The virtual Managed IP (MIP) address that is used by the Active Server for campus resiliency. The Active Server is always assigned to the MIP. If a switchover occurs the MIP is assigned to the new Active Server. Agents and other applications are not aware that a switchover has occurred because the IP address does not change. A MIP is only used when the Active and Standby Servers are in the same subnet.
Active Server details	The IP address for the server initially configured in Active mode.
Standby Server details	The IP address for the server initially configured in Standby mode.
Trusted IP address	The IP address of a trusted server that is not likely to go down so that both Active and Standby servers have something to ping regularly to verify the network connection.
Remote Geographic Node	The IP address of the optional Remote Geographic Node.

Configuring the hot-standby server

About this task

Configure a standby server for the active server.

Procedure

1. Log on to the server.
2. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
3. In the left pane of the High Availability window, expand **Configuration**.

4. Click **Server Mode**.
5. Under **Server Mode Configuration**, select **Standby**.
6. Click **Save**.

Important:

CCT SOA configuration (CCT Web services) information is not replicated to standby or RGN servers. Configure CCT Web services identically for the active CCT, the standby CCT, and the RGN server.

Variable definitions

Name	Description
Server Mode Configuration	The mode of the server: • Active: The server currently used to handle contacts. • Standby: The server used for back up operation if the active server fails.
Switchover	Determines whether Switchover is enabled and the length of time configured for server inactivity before a switchover to the Standby server for handling contacts. AACC replicates this information from the active server.
Managed IP	The IP address that is used for both the Active and Standby servers for campus resiliency.
Active Server details	The IP address for the server initially configured in Active mode.
Standby Server details	The IP address for the server initially configured in Standby mode.
Trusted IP address	The IP address of a trusted server that is not likely to go down so that both Active and Standby servers have a server to check to verify the network connection.

Disabling High Availability on a Hot-standby server

About this task

Disable the High Availability feature on each configured server.

Procedure

1. Log on to the standby server.

2. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
3. In the left pane of the High Availability window, expand **Tasks**.
4. Click **System Control** tab.
5. In the **Control** box, select **Shadowing**.
6. Click **Stop**.
7. In the left pane of the High Availability window, expand **Configuration**.
8. Click **System**.
9. Under **System**, select **Restore configuration**.
10. Click **Save**.
11. Configure server detail on the server.
12. Log on to the Active server.
13. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
14. In the left pane of the High Availability window, expand **Tasks**.
15. Click **CC Applications** tab.
16. In the **CC Applications** box, select **System**.
17. Click **Stop**. Ensure all contact center services are stopped before proceeding.
18. In the left pane of High Availability window, expand **Configuration**.
19. Click **System** tab.
20. Under **System**, select **Restore configuration**.
21. Click **Save**.
22. Configure server detail on the server.

Configuring the notification of automatic switchovers

Before you begin

- Configure the standby server with automatic switchover. See Configuring hot-standby managed IP address on page 492.
- If anonymous users are allowed, a username and password might not be required. Check with the Administrator of the email server for setup configuration.

About this task

Use the High Availability utility to send an email to a configured user.

Procedure

1. Log on to the active server.

2. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
3. In the left pane of the High Availability window, expand **Configuration**.
4. Click **Notifications**.
5. Under **Notification Level**, select an option for the notification.
6. If you choose email, in the **Hours** box, specify the number of hours to elapse between email message notifications.
7. Configure the **Notification Configuration** section to specify your SMTP server name, From Address, and To Address as applicable for your notification level.
8. Click **Save**.

Variable definitions

Name	Description
Email	Enable or disable email notifications.
SMTP	SMTP server name this is automatically verified when saving the data.
Username	The email User login name.
Password	The email User login password.
Charset	The email character set to use.
From Address	email address from which to send notifications.
To Address	email address to which to send notifications.
Hours	The interval, in hours, when an email is sent to the configured user if an automatic switchover has occurred.

Configuring hot-standby manual switchovers

Before you begin

- Configure the standby server for the Contact Center server (CCT, CCMS, or CCMM) you want to manually switch over. See Configuring hot standby managed IP address on page 492.

About this task

Configure a manual switchover from the active server to the standby server. You can manually start the standby server to operate in the active mode.

You can initiate a manual switchover only in the following situations:

- The active and standby servers are in running state.

- The active server is running. All the critical CCMS and CCT services are monitored and running.
- The active server has Switchover enabled.
- The shadowing latency is less than the threshold.
- A database restore is not running on the Standby server.
- The active server database and standby server database are synchronized. The standby server database is shadowing the active server database.
- The standby server can communicate with (ping) the Trusted IP address.

Procedure

1. Log on to the current active server.
2. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
3. In the left pane of the High Availability window, expand **Configuration**.
4. Double-click **Server Mode**.
5. Select **Switchover**.
6. Change the switchover time if required.

   The default switchover time is 60 seconds.
7. Click **Save**.

Configuring service monitoring

Before you begin

- Configure a standby server for each Contact Center server on which you want to configure automatic switchover. See Configuring hot-standby managed IP address on page 492.

About this task

The High Availability feature monitors a number of critical services on the Active Server. If any of these critical services stop or fail they are automatically restarted in the correct order. If a critical service fails a defined number of times then the Active Server can, if Switchover is enabled, shut down and hand over processing to the Standby Server.

These critical services are listed, monitored, restarted and controlled using the Contact Center Configuration dialog under the Tasks tab of the High Availability utility. It lists the critical CCMS services and all of the CCT services on the Voice Contact Server.

There is no requirement to change the data in this table, the default values are suitable for most solutions.

If the services are selected for Monitor and Restart and one or more services fail, either the same or more number of times as the Restart Limit value, then a switchover to the standby server occurs.

The HA service monitor uses its internal service restart counter to track the number of service restarts that have occurred for the monitored service. The number of restarts is limited to the Restart Limit configured in the High Availability Utility.

The service monitor triggers the switchover when the restart counter for the monitored service has reached the Restart Limit configured for the service, but only in the following situations:

- Switchovers are enabled on both active and standby servers.
- The standby server is shadowing the data from the active server.
- Both the active and standby servers have valid license files.

The service monitor resets its internal service restart counter to zero. This allows a restart of the monitored service when the Restart Limit is reached. The restart counter is reset to zero under one or more of the following conditions:

- After the Restart Threshold: 7200 seconds or configured value of threshold.
- When changes are made on the CC Configuration window in the High Availability Utility.
- The switchover fails. For example, when switchovers are not enabled on the standby server or the standby server is not shadowing data from the active server.
- The Restart check box is not selected on the CC Configuration window for the monitored service.
- Switchover is disabled on the active server.

The Restart Threshold is the time period within when the services are monitored and the counters are increased when services fail. When this threshold has been met the counters are reset to zero, and monitoring starts again as does the restart threshold timer.

Note:

This procedure does not apply to SIP-enabled contact centers.

Procedure

1. Log on to the server for which you want to configure the automatic switchover for services that fail.
2. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
3. In the left pane of the High Availability window, expand **Tasks**.
4. Double-click **CC Configuration**.
5. For each service, select the **Monitor** check box to monitor the service.
6. For each service, select the **Restart** check box to attempt to restart the service.
7. For each service, in the **Start Wait Time** column, type the number of seconds to wait before a service restarts.
8. For each service, in the **Stop Wait Time** column, type the number of seconds to wait before a service stops.
9. For each service, in the **Restart Limit** column, type the maximum number of attempts to restart the service before a switchover.

10. For each service, in the **Restart Threshold** column, type the time (in seconds) to reset the Restart Limit after the threshold is passed.
11. If changes are made to the CCT services, you must restart the server.

Variable definitions

Name	Description
CC	The Contact Center application name, CCMS, CCT.
Service	The application service name, for example the CCMS OAM_Service.
Monitor	Used to enable or disable the service monitoring.
Restart	Used to set up if the service needs to be restarted if it stops.
Start Wait Timer	The time in seconds that the service monitor waits before restarting or initiating a switchover to the standby server if this service is not running. The default CCT services *Start Wait Time* is 60 seconds. Do not configure the CCT services *Start Wait Time* to be less than 60 seconds.
Stop Wait Time	The waiting time (in seconds) for the next restart decision.
Restart Limit	The number of times a service can be restarted by the service monitor before initiating a switchover.
Restart Threshold	The time elapsed since the last restart of a call processing service by the Service Monitor. It is the time value in seconds to reset the Restart Counter to the value zero by the Service monitor.

Configuring hot standby automatic switchovers

Before you begin

- Configure a standby server for each active server on which you want to configure automatic switchover. See Configuring hot standby managed IP address on page 492.

About this task

Configure automatic switchover to automatically run the standby server if the active server fails or is shut down.

Note:

If you plan to reboot the active server as part of a planned activity, disable automatic **Switchover** and re-enable it after Avaya Aura® Contact Center services startup after the reboot.

Procedure

1. Log on to the active server for which you want to configure the automatic switchover for services that fail.
2. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
3. In the left pane of the High Availability window, expand **Configuration**.
4. Click **Server Mode**.
5. Select the **Switchover** check box.
6. Configure the number and unit of time until the automatic switchover.
7. Click **Save**.

Monitoring switchover information

About this task

Monitor the switchover information to determine why the automatic or manual switchover occurred.

Procedure

1. Log on to the server for which you want to review the switchover status.
2. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
3. In the left pane of the High Availability window, expand **Tasks**.
4. Select **System Control**.
5. Review the content of information in the **System Control** panel to determine why the switchover occurred.
6. In the **Control** box, select the status of the standby configuration.

Variable definitions

Name	Description
Control	Choose to maintain the current active server configuration, or switch back to the original configuration (switchback).

Procedure job aid

The configuration for the automatic switchover is cancelled when one automatic switchover completes. You must re-enable the automatic switchover. See Configuring hot standby automatic switchovers on page 499.

Reviewing shadowing

About this task

Review the server status to confirm that the shadowing is occurring between the servers.

Procedure

1. Log on to the server for which you want to review the switchover status.
2. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
3. In the left pane of the High Availability window, expand **Configuration**.
4. Select **System**.
5. In the **System** panel, locate the shadowing entries.
6. Confirm the last record of shadowing is within the last minute of the current time.
7. Click **Save**.

Configuring campus Mission Critical High Availability on the active server

About this task

Configure High Availability resiliency on a campus active server using the High Availability Utility. The active server is the Contact Center server that normally processes calls.

Procedure

1. Select one Contact Center server to be the active server, and log on.
2. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
3. Expand **Configuration**.
4. Double-click **Server Mode**.
5. Under **Server Mode**, select **Active**.

6. Under **Switchover And Network Timeout Configuration**, in the **Network Timeout** box, type the maximum length of time the network connectivity tests can continue to fail consecutively before corrective action is considered.
7. Under **Switchover And Network Timeout Configuration**, from the drop down list, select the unit of time for the network connectivity tests.
8. Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the active server.
9. Under **IP Configuration**, in the **Standby CLAN** box, type the IP address for the standby server.
10. Under **IP Configuration**, in the **Managed IP** box, type the Managed IP address.
11. Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server.
12. In the **Remote Geographic Node** box, type the IP address of the optional Remote Geographic Node.
13. Under **SMMC Port Configuration**, in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the local (active) server.
14. Under **SMMC Port Configuration**, in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the remote (standby) server.
15. Click **Save**.

Important:

CCT SOA configuration (CCT Web services) information is not replicated to standby or RGN servers. Configure CCT Web services identically for the active CCT, the standby CCT, and the RGN server.

Variable definitions

Name	Description
Network Timeout	The High Availability feature tests network connectivity between HA components by default every 100 milliseconds (100ms). The High Availability—Network Timeout value sets the maximum length of time these network connectivity tests can continue to fail consecutively before corrective action is considered. For example, if Network Timeout is set to 400ms, HA requires 4 consecutive failed network connectivity tests before the remote system is marked as unreachable. In this case, if switchovers are enabled, an attempt to switch over is made.

Table continues…

Name	Description
	Avaya recommends that you set Network Timeout high enough to be tolerant of normal network latency, but low enough to be responsive if a failure occurs.
Active CLAN	The IP address for the server initially configured in Active mode.
Standby CLAN	The IP address for the server initially configured in Standby mode.
Managed IP	The virtual Managed IP (MIP) address that is used by the Active Server for campus resiliency. A MIP is used only when the Active and Standby Servers are in the same subnet.
Trusted IP	The IP address of a trusted server that is not likely to go down so that both Active and Standby servers have a server to ping regularly to verify the network connection. Avaya recommends that you use an IP address from your IT infrastructure as the Trusted IP address.
Remote Geographic Node	The IP address of the optional Remote Geographic Node.
Local SMMC Port	The port number for System Management and Monitoring Component (SMMC) on the local (active) server. The default port number is 57012.
Remote SMMC Port	The port number for System Management and Monitoring Component (SMMC) on the remote (standby) server. The port number entered here must match the port number set on the remote (standby) server. The default port number is 57012.

Configuring Mission Critical High Availability on the Standby Server

Before you begin

- The Active Server databases are restored on to the Standby Server.

About this task

Configure High Availability resiliency on the Standby Server using the High Availability utility. The Standby Voice Contact Server shadows the Active Server and takes over processing if the Active Server fails.

Procedure

1. Log on to the Standby Server.
2. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
3. Expand **Configuration**.
4. Double-click **Server Mode**.
5. Under **Server Mode**, select **Standby**.
6. Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the active server.
7. Under **IP Configuration**, in the **Standby CLAN** box, type the IP address for the standby server.
8. Under **IP Configuration**, in the **Managed IP** box, type the managed IP address.
9. Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server.
10. Under **SMMC Port Configuration**, in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the remote (active) server.
11. Under **SMMC Port Configuration**, in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the local (standby) server.
12. Click **Save**.

Important:

CCT SOA configuration (CCT Web services) information is not replicated to standby or RGN servers. Configure CCT Web services identically for the active CCT, the standby CCT, and the RGN server.

Variable definitions

Name	Description
Active CLAN	The IP address for the server initially configured in Active mode.
Standby CLAN	The IP address for the server initially configured in Standby mode.
Managed IP	The virtual Managed IP (MIP) address that is used by the Active Server for campus resiliency. A MIP is used only when the Active and Standby Servers are in the same subnet.
Trusted IP	The IP address of a trusted server that is not likely to go down so that both Active and Standby servers

Table continues…

Name	Description
	have a server to ping regularly to verify the network connection. Avaya recommends that you use an IP address from your IT infrastructure as the Trusted IP address.
Local SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the local (standby) server. The default port number is 57012.
Remote SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the remote (active) server. The port number entered here must match the port number set on the remote (active) server. The default port number is 57012.

Starting a Mission Critical Active Server

About this task

Start the Active Server using the System Management and Monitoring Component (SMMC) system tray. Starting the Active Server starts Contact Center services and system processes.

Procedure

1. Log on to the Active Server.
2. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
3. Expand **Configuration**.
4. Under **Switchover And Network Timeout Configuration**, select **Enable Switchover**.
5. Click **OK**.
6. On the Windows taskbar of the active server, right-click on the **System Management and Monitoring Component (SMMC)** system tray, and select **Start HA System**.
7. To verify that the Contact Center services are running using the SCMU, select **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**. Check the Contact Center services are running.

Starting shadowing on a Mission Critical Standby Server

About this task

Start shadowing on the Standby Server using the System Management and Monitoring Component (SMMC) system tray.

The Standby Voice Contact Server shadows the Active CCMS and CCT server, maintaining a near real-time local copy of the CCMS, CCT, and Administration databases. The Standby Server is therefore configured with the most recent data and it can take over from the Active Server if necessary.

Procedure

1. Log on to the Standby Server.
2. On Windows taskbar of the standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**.
3. To verify that the Contact Center services are running using the SCMU, select **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**. Check the CCMS and CCT services are running.

Stopping High Availability on a Mission Critical Standby Server

About this task

Stop shadowing and disable High Availability on a Standby Server using the System Management and Monitoring Component (SMMC) system tray.

Procedure

1. Log on to the Standby Server.
2. On Windows taskbar of the Standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Stop HA System**.
3. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
4. Expand **Configuration**.
5. Double-click **Server Mode**.
6. Under **Server Mode**, select **Non HA**.
7. Click **Save**.

Stopping High Availability on a Mission Critical Active Server

About this task

Stop shadowing and disable High Availability on an Active Server using the System Management and Monitoring Component (SMMC) system tray.

Procedure

1. Log on to the Active Server.
2. On Windows taskbar of the Active server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Stop HA System**.
3. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
4. Expand **Configuration**.
5. Double-click **Server Mode**.
6. Under **Server Mode**, select **Non HA**.
7. Click **Save**.

Disabling Auto Startup on a Mission Critical server after reboot

About this task

Disable your Mission Critical server from automatically starting Avaya Aura® Contact Center services after you reboot the server.

This procedure applies to both Active and Standby servers.

Procedure

1. Log on to the Active or Standby server.
2. On the Windows taskbar of the server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Disable Next Auto Startup**.

Selecting a startup mode on the Mission Critical Standby server after reboot

About this task

Select a startup mode for your Standby server. You can choose from the following options:

- **Full HA Startup**. If you choose this option, after a system reboot, SMMC starts all services and starts shadowing the Active server.
- **Shadowing Only Startup**. If you choose this option, after a system reboot, SMMC does not start services but starts shadowing the Active server.

Procedure

1. Log on to the Standby server.
2. On the Windows taskbar of the Standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Select Standby Auto Startup Mode**.
3. Select **Full HA Startup** or **Shadowing Only Startup**.

Re-enabling High Availability after stopping services

About this task

This procedure applies only when the HA state of the active server in the SMMC system tray is running but with switchovers disabled. This state occurs when you stop a critical service on the active server using System Control and Monitor Utility (SCMU).

Re-enable High Availability to ensure all services are started and your active HA server is in running state.

Procedure

1. Log on to the active server.
2. On the Windows taskbar of the server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Re-enable HA System**.

   All services are now started and the active HA server is in running state.

Reinstating Mission Critical High Availability

About this task

In a Mission Critical High Availability campus solution, there are two types of switchovers, managed or unmanaged. A managed switchover is one initiated by the administrator or caused by

a failure of a monitored CCMS or CCT service. An unmanaged switchover results from a hardware, network, database, or power failure. After the switchover, the standby node is now active, and is running the contact center call routing. After the switchover, the active node is now in standby mode and is either stopped, or in the process of stopping.

To make your servers High Availability (HA) capable again, you must perform some steps on both the new active and standby servers.

If you use a Remote Geographic Node, your standby server does not have an active instance of Contact Center License Manager. Therefore you cannot run your contact center for an extended period of time on the standby server. After reinstating High Availability, perform a manual switchover as soon as possible, to ensure that the original active server can process license requests.

Procedure

1. On to the new standby server, from the System Management and Monitoring Component (SMMC) system tray, click **Start HA System**.
2. If the new Standby server is not synchronized with the Active server, a dialog box appears with a message to restore the active server databases.
3. If a dialog box showed a message to restore the active server databases, back up the active server databases and restore them on the standby server:
    a. On the new active server, run the Database Maintenance utility and back up all of the database applications, including Offline where present, to a network share. You do not have to stop the services on the active server to perform this back up.
    b. On the new standby server, from the System Management and Monitoring Component (SMMC) system tray, click **Stop HA System**.
    c. Run the Database Maintenance utility and restore each database application, including Offline where present, from the network share.
4. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
5. On the Server Mode dialog, confirm that the server mode is Standby, and that the IP address information is correct.
6. Click **Save**.
7. Close the High Availability configuration utility.
8. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
9. In the left pane, select **Local Settings**.
10. Ensure that the CLAN Subnet IP Address matches the IP address of the new standby server.
11. Click **Apply All**.
12. On the Restart Required dialog, click **No**.
13. Click **Exit**.
14. On the new standby server, from the System Management and Monitoring Component (SMMC) system tray, click **Start HA System**.

15. On the new active server, from the System Management and Monitoring Component (SMMC) system tray, click **Enable Switchover**.
16. If your HA solution supports multimedia contacts, on the primary Contact Center Multimedia server, restart the CCMM Multimedia Contact Manager service.

Reinstating Hot Standby High Availability

About this task

Switchovers result from network or power outages, or critical monitored service termination on an active node in your contact center. After the switchover, the standby node is now active, and is running the contact center call routing. After the switchover, the active node is now in standby mode and is either stopped, or in the process of stopping.

To make your servers High Availability (HA) capable again, you must perform some steps on both the new active and standby servers.

Procedure

1. If the High Availability Utility displays a message stating that a database restore to the new Standby server is required:
   a. On the new active server, run the Database Maintenance utility and back up all of the database applications, including Offline where present, to a network share.

      You do not have to stop the services on the active server to perform this back up.

   b. On to the new standby server, run the Database Maintenance utility and restore each database application, including Offline where present, individually from the network share.
2. On to the new standby server, run the Server Configuration utility to update the Local CLAN information to identify the real local IP address.
3. If you are asked to reboot, a reboot of the server is not necessary.
4. In the Server Configuration utility, click **Apply All**.
5. Click **OK**.
6. Click **Exit**.
7. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
8. On the Server Mode dialog, click **Save**.
9. Close HA configuration utility.
10. Log on to the new standby server.
11. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
12. Click **Tasks** > **System Control**.

13. Select **Shadowing**.
14. Click **Start**.
15. Click **OK** to close HA configuration utility.

Reinstating High Availability on a Multimedia Contact Server Only

About this task

A switchover results from a network or power outage, or critical monitored service termination on an active CCMM server in your contact center. After a switchover, the standby CCMM server is now active, and is processing multimedia contacts. After a switchover, the active CCMM server is now in standby mode and is either stopped, or in the process of stopping.

To make your Multimedia Contact Server Only servers High Availability (HA) capable again, you must perform some steps on both the new active CCMM and standby CCMM servers.

Procedure

1. If the High Availability Utility displays a message stating that a database restore to the new Standby server is required:
    a. On the new active CCMM server, run the Database Maintenance utility and back up all of the database applications, including Offline, to a network share.

       You do not have to stop the services on the active server to perform this back up.

    b. On to the new standby CCMM server, run the Database Maintenance utility and restore each database application, including Offline, individually from the network share.
2. Log on to the new standby CCMM server.
3. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
4. Under **Server Mode Configuration**, select **Switchover**.
5. Click **Save**.
6. Click **Tasks** > **System Control**.
7. Select **Shadowing**.
8. Click **Start**.
9. Click **Exit**.
10. Log on to the new active CCMM server.
11. On the **Apps** screen, in the **Avaya** section, select **High Availability**.
12. Under **Server Mode Configuration**, ensure that **Switchover** is checked.

13. Click **Save**.
14. Click **Exit**.

How to manually switch over to a Remote Geographic Node

Before you begin

- Ensure the Remote Geographic Node (RGN) is configured to use a local Avaya Aura® Unified Communications voice platform.

About this task

If the High Availability campus site fails or is shutdown, you can manually start your Remote Geographic Node solution. During normal operation the Remote Geographic Node (RGN) shadows the campus site database. The RGN is configured to use local voice platform and multimedia resources. The RGN is configured with the same agent and skillset information as the campus site. If the campus site fails or is shutdown, you must start the RGN Contact Center and Avaya Agent Desktop applications.

Important:

Before you start your Remote Geographic Node solution, you must ensure that all campus AACC components are shut down or removed from the network. RGN operation can be impacted if any campus AACC components are active when the RGN starts.

Complete this procedure to commission the Remote Geographic Node to handle voice and multimedia contacts. The Remote Geographic Node also supports local reporting.

Procedure

1. On the Remote Geographic Node (RGN), use the System Management and Monitoring Component (SMMC) system tray to stop the High Availability system.
   a. On Windows taskbar of the RGN server, right-click on the SMMC system tray, and select **Stop HA System**.
   b. This ensures that the Remote Geographic Node server is not attempting to shadow data from the faulty or stopped campus site.
2. On the RGN server, using the High Availability configuration utility, temporarily set the server to the non-HA mode.
   a. On the RGN server, open the High Availability configuration utility.
   b. Expand **Configuration**.
   c. Double-click **Server Mode**.
   d. Under **Server Mode**, select **Temporarily set as non-HA**.
   e. Reboot the server when prompted.

3. On the RGN server, use the SMMC system tray to start Contact Center services if required.
    a. On Windows taskbar of the RGN server, right-click on the SMMC system tray, and select **Start System**.
    b. The Contact Center services begin to start in the correct order.
4. On the RGN server, use the System Control and Monitor Utility (SCMU) to verify that all core Contact Center services started.
    a. On the **Apps** screen, in the **Avaya** section, select **System Control and Monitor Utility**.
    b. Click the **Contact Center** tab, and verify that the services have started.
5. Log on to CCMA and confirm that the CCMS, CCT, and optional CCMM server information has updated with the RGN IP and server name details.
6. On the Avaya Aura® Media Server primary node of the RGN site, in Element Manager, click **Cluster Configuration** > **Replication Settings**. Clear the **Master Cluster Primary Node Address** option. This stops the RGN site from attempting to replicate content from the primary Avaya Aura® Media Server data center on the campus site.
7. Log on to the RGN CCMA. From the CCMA **Launchpad**, select **Configuration**, and then **Media Servers**. Ensure that the **Master Content Store** option is selected for the local RGN Avaya Aura® Media Server or the local RGN Avaya Aura® Media Server HA pair.
8. Launch Avaya Agent Desktop clients using the RGN Voice and Multimedia Contact Server host name. For more information about launching Agent Desktop, see *Using Agent Desktop for Avaya Aura® Contact Center* .

How to revert to a campus site after running the RGN

About this task

If a campus site fails or is shutdown, you can manually start your Remote Geographic Node solution. You can then use the Remote Geographic Node (RGN) servers until the campus site is available again. When the campus is available, you must shut down the RGN servers and re-enable the campus site. Before you back up the RGN database you must stop the RGN server. Do not start the RGN server until you configure campus and RGN HA once again. This ensures that the data restored to the campus site is consistent.

In the following example the remote site has an RGN Voice and Multimedia Contact Server, and a single local standalone Avaya Aura® Media Server. The campus site has a HA pair comprising an active server and a standby server. If you have a single server at the campus site, ignore the instructions relating to the standby server.

Complete this procedure to commission the campus site to handle voice and multimedia contacts.

Procedure

1. On the Remote Geographic Node (RGN), use the System Management and Monitoring Component (SMMC) system tray to stop the Contact Center.
   a. On Windows taskbar of the RGN server, right-click on the SMMC system tray, and select **Stop HA System**.
   b. The Contact Center services on the RGN server begin to stop in the correct order.
2. On the RGN server, backup all the application databases and the ADMIN database.
   a. On the RGN server, open the Contact Center Database Maintenance utility.
   b. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Backup Locations**.
   c. In the right pane, click **Create**.

      Note:

      If there is a backup location already available, you do not need to create a new backup location.

   d. On the warning dialog box, click **Yes**.
   e. From the **Drive Letter** list, select the network drive on which to store the Voice and Multimedia Contact Server database.
   f. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Folder\Backup Location.
   g. In the **Username** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
   h. In the **Password** box, type the user password.
   i. Click **Save**.
   j. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Immediate Backup**.
   k. In the **Media Type** section, select **Network Location**.
   l. In the **Application** section, if you have Voice and Multimedia Contact Server, select **Offline**.
   m. From the **Backup Location** list, select the network drive on which to store the backup.
   n. Click **Backup**.
   o. Click **Yes**, to continue with the backup.

      Backups can take some time to complete, depending on the size of the database.

   p. When the backup completes, click **OK**.
3. On the campus active server, restore the RGN database backups.

Note:

If the RGN database backup is saved to a location not previously created on the active server, you must create the backup location.

a. On the campus active server, open the Contact Center Database Maintenance utility.
b. In the Contact Center Database Maintenance window, in the Main Menu pane, click **Restore**.
c. In the **Media Type** section, select **Network Location**.
d. In the **Application** section, select **CCT**, **CCMS**, **CCMM**, **CCMA** and **ADMIN**.
e. In the **Restore contents** section, select **Data** and **Offline**.
f. From the **Backup Location** list, select the network drive containing the backed up RGN databases.
g. Click **Restore**.
h. Use the **Progress information** field to monitor the progress of the restoration.

   Restores can take some time to complete, depending on the size of the database.
i. On the **Database Maintenance** message box, click **OK**.
j. Open **Server Configuration**, click **Apply All**, and reboot the server.

4. On the RGN, using the High Availability configuration utility, put the RGN server back into RGN mode.
   a. On the RGN server, open the High Availability configuration utility.
   b. Expand **Configuration**.
   c. Double-click **Server Mode**.
   d. Under **Server Mode**, clear **Temporarily set as non-HA**.
   e. Click **Save**.
   f. Click **OK** and reboot the RGN server.
5. On the active server, use the SMMC system tray to start the active server if required.
   a. On Windows taskbar of the active server, right-click on the SMMC system tray, and select **Start HA System**.
   b. The Contact Center services on the active server begin to start in the correct order.
6. After the active server is up and all services are running, log on to CCMA.
7. During the first CCMA logon session, CCMA presents a *RGN Information* message box requesting confirmation to change CCMS, CCT, and CCMM server names back to the original campus values. Click Yes to accept the recommended changes.
8. Backup the active server databases and restore them to the standby server and the RGN server. Re-enable and restart High Availability on the standby server and RGN server. For more information, see the High Availability commissioning chapters in *Avaya Aura® Contact Center Commissioning for Avaya Aura® Unified Communications*.

9. If you made changes to the voice prompts at the RGN site that now need to be replicated back to the primary data center, you must temporarily force the primary data center Master cluster to replicate content from the RGN Avaya Aura® Media Server or RGN Master cluster. Perform these steps to temporarily force the campus Avaya Aura® Media Servers to replicate from the RGN primary Avaya Aura® Media Server:
    a. At the campus site, on the primary data center Avaya Aura® Media Server Master cluster primary node, log on to Element Manager.
    b. In Element Manager click **Cluster Configuration** > **Replication Settings**, and configure the **Master Cluster Primary Node Address** field to the address of the RGN Master cluster primary node.
    c. View the Element Status page and wait for any synchronization alarm conditions to clear. This can take a few moments unless you have large volumes of content in your content store. Depending on the amount of media content in your solution, you might not even observe alarms.
    d. View the content for your SIP domain namespace in the Media Management page to confirm that expected updates have replicated successfully.
    e. In Element Manager, clear the **Master Cluster Primary Node Address** field. Your Avaya Aura® Media Servers at the campus site now have the same voice prompts as the Avaya Aura® Media Servers at the RGN site.
10. When reverting to the campus site, you must configure Avaya Aura® Media Server content replication settings to allow voice prompt administration to be performed at the primary data center at the campus site. You must also ensure that the voice prompt content replicates to the Avaya Aura® Media Servers at the RGN site. Perform these steps to configure voice prompt administration at the primary data center at the campus site:
    a. At the RGN site, on the Avaya Aura® Media Server primary node of the RGN Master cluster, set the **Master Cluster Primary Node Address** field to the address of the primary data center Master cluster primary node.
    b. At the campus site, from the CCMA Launchpad, select Configuration, and then Media Servers. Select the primary Avaya Aura® Media Server or the primary Avaya Aura® Media Server HA pair and ensure that the **Master Content Store** option is selected. This Avaya Aura® Media Server or Avaya Aura® Media Server HA pair now manages the voice prompts in your solution when the campus site is running.

How to manually switch over to the Remote Geographic Node in an AML CS1000-based solution

If the CS1000 AML-based Hot-standby High Availability campus site fails or is shut down, you can manually commission and start the Remote Geographic Node solution. During normal operation the Remote Geographic Node (RGN) shadows the campus site database. The RGN therefore has the same configuration as the campus site. The RGN has the correct configuration of agent and skillset information, the same as the campus site.

You can manually commission the RGN servers by ensuring the server configuration details point to local telephony and multimedia resources at the RGN location.

In the following example the geographic site has a Remote Geographic Node Voice Contact Server and a Remote Geographic Node Multimedia Contact Server.

Before commissioning the Remote Geographic Node server:

- Completely disable the active and standby servers on the campus site.
- Activate the Avaya Communication Server 1000 (CS1000) Survivable Media Gateway on the geographic site.

Remote Geographic Node CCMS, CCMA, and CCT configuration

Perform the following steps on the Remote Geographic Node (RGN) Voice Contact Server:

- Use the HA utility to verify that shadowing has stopped. Stop shadowing if it has not.
- Use the HA utility to select, while in RGN server mode, the **Temporarily set as non-HA** check box, and click **OK**.
- Use the System Control and Monitor Utility (SCMU) to start all services.
- Log on to the RGN CCMA Web administration, and manually update the CCMS, CCT, and CCMM servers to the RGN server name and IP address.
- Start Agent Desktop.
- If your Contact Center solution uses an external Web Communications server, configure the Web Communications server to update the files with the RGN server name.
- If your Contact Center solution uses Proactive Outreach Manager (POM), configure the POM server to point to the RGN server.

How to revert to the campus site after running the RGN for a few days

If a Hot-standby High Availability campus site fails or is shut down, you can manually commission and start the Remote Geographic Node solution. You can then use the Remote Geographic Node (RGN) servers until the campus site is available again. When the campus servers are available you must shutdown the RGN servers and re-configure High Availability on the campus site. Avaya Aura® Contact Center is out-of-service during this re-configuration period, because the campus HA servers must be rebuilt with consistent data, without any configuration or statistical data updates on the RGN server that might not get restored on the new campus HA server.

In the following example the solution has a HA pair of Voice Contact Servers at the campus, and a Remote Geographic Node Voice Contact Server.

- Stop shadowing, and stop all contact center services on the RGN server.
- On the RGN server, backup all the application databases and the ADMIN database.

- On the RGN server, using the High Availability utility, ensure that shadowing is stopped and clear the **Temporarily set as non-HA** check box. This sets the RGN server back to RGN mode.
- Restore the RGN database backups on the campus active server.
- On the campus active server, using the High Availability utility, under **Tasks** > **CC Applications**, click **Start** to start HA. This starts the AACC services.
- Use the System Control and Monitor Utility (SCMU) to confirm that all services started.
- Log on to CCMA, and manually update the CCMS, CCT, and CCMM server names to the original campus values.
- After the active server is up, take a database backup from the active server, and restore this backup to both the standby server and the RGN server.
- On the standby and RGN servers, using the High Availability utility, start shadowing.

Chapter 45: Common procedures

This chapter describes the common procedures that you perform to administer your Avaya Aura® Contact Center software.

Starting or stopping Contact Center applications

Before you begin

Important:

When you start the System Control and Monitor Utility, there is a delay before RptAdmin shows as started. This is expected behavior and the RptAdmin status corrects itself within a short time.

About this task

Use the System Control and Monitor Utility to start and stop all of the applications in Contact Center.

Procedure

1. Log on to the server on which the Contact Center applications to start or stop are installed.
2. On the **Apps** screen, in the **Avaya** section, select **System Control and Monitor Utility**.
3. Click the **Contact Center** tab.
4. Select the check box for each application to start or stop on the current server.
5. To start the selected applications, click **Start Contact Center**.

   OR

   To stop the selected applications, click **Shut down Contact Center**.

Part 11: Server name or IP address change

- Server name or IP address change on page 521
- Voice and Multimedia Contact Server name change on page 524
- Voice and Multimedia Contact Server IP address change on page 538
- Voice Contact Server name change on page 546
- Voice Contact Server IP address change on page 558
- Multimedia Contact Server name change on page 566
- Multimedia Contact Server IP address change on page 576
- Avaya Aura Media Server server name change on page 579
- Avaya Aura Media Server IP address change on page 582

Chapter 46: Server name or IP address change

To change the server name or an IP address of a server already running in your contact center, you must perform the procedures in this chapter to ensure that your servers in the Avaya Aura® Contact Center suite are updated with the correct information.

You can change the name of a server with CCMS, CCMA, CCT, Avaya Aura® Media Server, or CCMM software installed. However, this is time consuming, so Avaya recommends that you configure the final production name of the server before installing Contact Center software.

Note:

You must stop Avaya Aura® Contact Center before changing the name or IP address of a Contact Center server.

Server name change and security certificates

If you change the name of a secured Contact Center server, Avaya recommends that you create a new security store with a server certificate that matches the new server name.

Each server certificate has a name, which normally derives from the server Fully Qualified Domain Name (FQDN). If a server certificate name does not match the name of the website or web service to which a client connects, the client generates a warning. Normally on a GUI, a user can bypass the warning and continue. If the client is a service on another system, it does not handle and bypass the warning unless coded to do so.

If you change the server name and do not change the server certificate, users always see warnings when they connect to Contact Center web services.

Solutions that require server certificates

- SIP-enabled solutions with an Avaya Unified Communications platform. These solutions always use TLS security for the CTI link to the AES.
- Solutions using the Agent Browser application. These always use TLS security for the Agent Browser application client.
- Solutions on which you enabled Web Services security.
- Solutions using Secure Real Time Protocol for voice traffic.

Preparing a server certificate before changing the server name

If you use an external Certificate Authority (CA), it can sometimes take an extended period to receive a signed server certificate after submitting your Certificate Signing Request (CSR) to the CA. To minimize the time elapsed for a server name change, you can create a CSR and request and receive a new server certificate before changing the server name. The following high-level procedures outline how to create a new CSR to send to the CA. For full details of these procedures, see *Avaya Aura® Contact Center Server Administration*.

Important:

If the CA you use to sign the new server certificate is different to the CA you used to sign the old server certificate, you must also distribute a new root certificate to all the relevant clients and servers after changing the server name and applying the new server certificate.

To create a new CSR in the Contact Center security store using Security Manager:

- Schedule a maintenance window for this task, because you must stop the Contact Center services.
- In Security Manager, back up the Contact Center security store.
- Delete the existing security store.
- Create a new security store, specifying the planned new server name as the common name for the certificate.
- Copy the CSR content from the new security store, to send to the CA to request a server certificate.
- Restore the Contact Center security store that you backed up.

You can now use the CSR you generated to request a server certificate from a CA. When the CA provides the new server certificate, you can schedule the Contact Center server name change.

In Avaya Aura® Media Server, you can create a new CSR at any time without stopping the server or impacting the existing certificates. Create a new CSR to request a new server certificate from a CA. When the CA provides the new server certificate, you can schedule the server name change.

High Availability solution server renaming considerations

About this task

In High Availability solutions, Avaya recommends that you store database backups on a remote server. Do not store database backups on the active or standby server.

- If the remote server storing the active server database backups is renamed, and the active server is offline for less than 24 hours, update the database location on the active server. This new server name is shadowed across to the standby server. The standby server can then restore the database from the remote location, if the active server fails.
- If the remote server storing the active server database backups is renamed and the active server is offline for more than 24 hours, the active server must be updated manually with the new location. Database shadowing stops working if the difference between the active and standby server database content is greater than 24 hours, so the standby server is not updated with this new backup location. In this case, using the High Availability utility, on the

standby server, change the standby server to be the active server and then change the database backup location manually. Perform a database restore and reset the server to be the standby server again. Start High Availability on the active server.

Prerequisites for changing server names or IP addresses

Procedure

- Understand if your network administrator is using a Domain Name Service in your network or if you need to update the HOSTS files on each server when you perform a name or IP address change.
- Know the old server name or IP address for your server and the new server name or IP address for your server.
- Ensure that your server name meets the requirements for the Contact Center server.
- If you are changing the Contact Center server IP address in a virtualized solution using WebLM, you must request a new license. Your existing license is no longer valid after you change the IP address.

Chapter 47: Voice and Multimedia Contact Server name change

Change the name of the Voice and Multimedia Contact Server where Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, Contact Center Multimedia, and other components are installed on the same server and update the properties of all other servers in the Contact Center Suite. The new name of the server must meet the specifications of the server names in the Contact Center suite.

Note:

You can use this chapter to change the name of the Voice and Multimedia Contact Server with Avaya Aura® Media Server server.

Voice and Multimedia Contact Server name change prerequisites

Procedure

- Ensure that the new server name is unique among both the domain and the other servers on the domain.
- Ensure that the new server name is from 6 to 15 characters and that the first character is alphabetical.
- Ensure that the new server name contains no underscores (_), spaces ( ), or punctuation.

Turning off Web Services security

About this task

Turn off Web Services security before you rename the server. If Web Services security is not enabled on your contact center, you can skip this procedure.

Procedure

1. Log on to the Contact Center server as a local administrator.

Important:

If you log on to the server as a domain administrator, this procedure does not complete successfully.

2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the password for the security store, and click **OK**.
4. On the Security Manager screen, select the **Security Configuration** tab.
5. Click **Security Off**.
6. Click **Apply**.
7. On the Security Change Confirmation dialog, click **Confirm**.
8. Click **Log Out**.
9. Restart the Contact Center server.

Changing the server name in the operating system

About this task

Change the server name on the Voice and Multimedia Contact Server operating system to the new server name.

Procedure

1. Log on to the Voice and Multimedia Contact Server as administrator.
2. On the Voice and Multimedia Contact Server, on the **Start** screen, select **Control Panel**.
3. On the Control Panel screen, click **System and Security**.
4. On the System and Security screen, click **System**.
5. In the **Computer name, domain, and workgroup settings** section, click **Change settings**.
6. Click the **Computer Name** tab.
7. Click **Change**.
8. Type the new server name.
9. Click **OK**.
10. Click **OK**.
11. Click **Close**.
12. Click **Restart Later**.

Important:

Do not restart the server until you synchronize the operating system name with the Voice and Multimedia Contact Server name. See Synchronizing the operating system name with the Voice and Multimedia Contact Server name on page 526.

13. If you are using a Domain Name Service, contact your local network prime to update the DNS with the new server name.

Verifying the server name change

Before you begin

- Ensure that you use a Domain Name Service server in your network.

About this task

Verify that the Domain Name Service server or network has the correct server name.

Procedure

1. Right-click **Start**.
2. Select **Run**.
3. Type `cmd`.
4. Click **OK**.
5. In a Command line window, enter `ping <server name>`.

   Where *<server name>* is the new name of the server.
6. Verify that the IP address matches the IP address of the server with the new name.

Synchronizing the operating system name with the Voice and Multimedia Contact Server name

About this task

Synchronize the operating system name with the Voice and Multimedia Contact Server name to ensure that the Contact Center suite uses the new server name.

Procedure

1. Log on to the Voice and Multimedia Contact Server as administrator.
2. Close the **System Control and Monitor Utility** if it is running.
3. On the **Apps** screen, in the **Avaya** section, select **Computer Update Utility**.

4. On the Contact Center Computer Name Synchronization Utility, click **OK**.

   If the names do not match, Contact Center prompts you to synchronize the names.

5. After the Voice and Multimedia Contact Server services shut down and the synchronize process completes, click **OK**.
6. On the Synchronization Utility box, click **OK**.
7. Restart the server.

Configuring the server name details

About this task

You must perform the following steps to update the server name references used by Contact Center.

Procedure

1. Log on to the contact center server.
2. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
3. Click the **Local Settings** tab.
4. Verify the server name details.
5. Click **Apply All**.
6. On the **Restart Required** dialog, click **Yes** to restart the server.

Joining the server to the domain

About this task

If you are using a domain and a DNS, you join the Voice and Multimedia Contact Server to the domain. This ensures that all servers can interpret the new server name.

Procedure

1. Log on to the DNS server.
2. On the DNS server, change the server name or IP address of the Contact Center server.
3. Remove the Contact Center server from the domain.
4. Join the Contact Center server back to the domain using the new server name and IP address.

Updating the HOSTS file on the Voice and Multimedia Contact Server

Before you begin

- Determine if you need to update the HOSTS table on your server.

Important:

Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2012 Release 2.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on the Voice and Multimedia Contact Server with the new server name and IP address. This ensures that all servers can interpret the new server name.

Procedure

1. Log on to the Voice and Multimedia Contact Server server.
2. Browse to the HOSTS file in the Windows Server 2012 Release 2 installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the file to reflect the new server name.
5. On the **File** menu, click **Save**.
6. Close all windows.

Resetting the iceAdmin password

Before you begin

- Obtain the domain account name and password from your network administrator, if your Contact Center server is a member of an active domain.

About this task

Contact Center Manager Administration uses the iceAdmin account. Reset the iceAdmin password to access the contents of the Administration database.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Manager Administration Configuration**.

3. In the left pane, click **Avaya**.
4. In the Avaya Applications Configuration window, click **IceAdmin Password Change**.
5. In the **Old Password** box, type the old password.
6. In the **New Password** box, type the new password for the iceAdmin user account.
7. In the **Confirm Password** box, type the password again.

   If your server is a member of an active domain, the Domain Account option is enabled in the iceAdmin Password Change window.
8. To export scheduled reports to a domain network PC, click **Domain Account**.
9. From the **Select Domain Name** list, select the name of the domain to add.
10. In the **Enter Domain Account** box, type the domain account.
11. In the **Enter Domain Account Password** box, type the domain account password.
12. In the **Confirm Domain Account Password** box, type the domain account password again.
13. Click **OK**.
14. Click **OK**.

Configuring destination for exported scheduled reports

Before you begin

- Plan to export scheduled reports to a computer on your domain network.

About this task

If you export scheduled reports to a domain network computer, configure the destination for exported scheduled reports.

Procedure

1. Log on to the server.
2. Create a folder. Name the folder **Exported Reports**.
3. Right-click the new folder and select **Properties**.
4. In the **Properties** dialog box, on the **Sharing** page, click **Advanced Sharing**.
5. Select **Share this folder**.
6. Click **Permissions**.
7. Click **Add**.
8. In the **Select Users or Groups** dialog box, click **Advanced**.

If Windows Sever 2012 prompts you for an account, enter an account with domain administrative privileges, and enter the account password.

9. Click **Find Now**.
10. In the expanded portion of the **Select Users or Groups** dialog box, locate and select the CCMA administrative account.
11. Click **OK**.
12. In the **Select Users or Groups** dialog box, click **OK**.
13. In the **Permissions** dialog box, select the CCMA administrative account.
14. Select the **Allow** check box for the following:
    - **Change**
    - **Read**
15. Click **Apply**.
16. Click **OK** to close the **Permissions for Exported Reports** dialog box.
17. Click **OK** to close the **Advanced Sharing** dialog box.
18. Click **Close** to close the **Exported Reports Properties** dialog box.

Reconfiguring security certificates after changing the server name

About this task

Re-configure the server security certificates after you change the server name. Complete the following tasks to update the Contact Center security store. For detailed steps on changing the Contact Center security store, see Contact Center security certificates administration on page 447

Procedure

1. Back up the Contact Center security store.
2. Delete the security store.
3. Create a new security store, using the new name of the server.
4. Use the Certificate Signing Request (CSR) from the new store to get a signed server certificate from a Certificate Authority (CA). Alternatively, if you created a new security store and received a certificate before changing the server name, restore that security store. For more information, see Server name change and security certificates on page 521.
5. Import the new signed server certificate and root certificate to the security store.

6. If the CA you used to sign the new server certificate is different to the CA you used to sign the old server certificate, export the new root certificate and distribute it to all the relevant clients and servers.

Changing the server name in the Administration tool

About this task

Change the Contact Center Manager Server name details in the Administration tool to ensure that Contact Center Manager Administration connects to the correct server.

Procedure

1. Log on to the Contact Center Manager Administration application as an administrator with all access permissions.
2. Click **Configuration**.
3. In the left pane, right-click the Contact Center Manager Server name to change.
4. Click **Edit Properties**.
5. Type the new server name, and click **Submit**.

Changing the CCT server name in the Administration tool

About this task

Update the CCT name in the CCMA configuration to ensure that the CCT Web administration launches correctly. Use CCMA to open the CCT Web administration utility.

Procedure

1. Log on to Contact Center Manager Administration.
2. Click **Configuration**.
3. From the **Server** menu, select **CCT Server**.
4. Right-click **CCT Server**, and then click **Edit Properties**.
5. Type the name of the new CCT Server name. Type the new name of this server.

   The system resolves the new CCT server name.
6. Click **Submit**.

Changing the CCMA and CCMM server name in the Dashboard

About this task

Change server names in the CCMM Dashboard to ensure that the CCMM Web administration utility launches.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Multimedia Dashboard**.
3. On the Multimedia Dashboard, under **Server Availability**, right-click **Contact Center Manager Administration** and select **Edit**.
4. On the **Administrator Login** dialog, in the **User Name** box, type `GeneralAdmin`.
5. In the **Password** box, type the password. The default password is "__ccmm!".
6. Click **Login**.
7. On the **Administrator Login** dialog, in the text box, type the name for the current Contact Center Manager Administration server.
8. Click **Save**.
9. On the Multimedia Dashboard, under **Server Availability**, right-click **Contact Center Multimedia Server** and select **Edit**.
10. On the **Administrator Login** dialog, in the **User Name** box, type `GeneralAdmin`.
11. In the **Password** box, type the password. The default password is "__ccmm!".
12. Click **Login**.
13. On the **Administrator Login** dialog, in the text box, type the name for the current Contact Center Multimedia server.
14. Click **Save**.

Changing the CCMM server name in the Administration tool

About this task

Update the CCMM name in the CCMA configuration to ensure that the CCMM launches correctly.

Procedure

1. Log on to Contact Center Manager Administration.

2. Click **Configuration**.
3. From the **Server** menu, select **CCMM Server**.
4. Right-click **CCMM Server**, and then click **Edit Properties**.
5. Type the name of the new CCMM Server. Type the new name for the server.

   The system resolves the new CCMM server name.
6. Click **Submit**.

Updating the email attachment folders

Before you begin

- Ensure that you have the email feature installed and enabled using the Contact Center License Manager.

About this task

Update the email attachment folders for Contact Center Multimedia. If you are licensed for email messages in your contact center, you must update the email attachment folders.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, from the **CCMM Servers** list, select your CCMM server.
3. Click **Launch Multimedia Client**.

   The CCMM Administration utility opens.
4. In the left column of the CCMM Administration utility, select **E-mail**.
5. Select **General Settings**.
6. In the **Attachment Files** area, update the path to match the new server path.
7. Click **Save**.

Configuring the external Web Communications server

Before you begin

- Know the custom interface folder names and paths for the web.xml and .jsp files for the sample Web communications installation.

About this task

If your solution uses an external Web Communications server, configure the Web Communications server to update the files with the new server name.

You must update for .jsp files with Apache Tomcat. If you use a different servlet engine (for example, JRun or WebLogic) or a different technology (ASP.NET), you must use the standard procedures for your environment.

Procedure

1. Log on to your external Web Communications Web server.
2. Open the config file located at `C:\xampp\htdocs\Code\include` in Notepad or another text editor.
3. Locate the text string CCMM_MACHINE_NAME and update the new server name after the '=' sign.
4. Save and close the file.

Updating shared folders for reports

Before you begin

- Ensure that you export scheduled reports in your Contact Center.
- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server (CCMS) name or that you updated the HOSTS file on the clients with the new CCMS name.

Important:

Administrators cannot update the browsers and shared folders for each user, therefore users need to update their respective browsers and shared folders.

About this task

Update the shared folders used for reports to reference the new Contact Center Manager Administration (CCMA) server name in the browser.

Procedure

1. Log on to the server.
2. Log on to the CCMA application as an administrator with all access permissions.
3. Click **Historical Reporting**.
4. In the Historical Reporting main window, on the system tree, click the server under which you want to modify the reports.
5. For each report associated with the new server, click the report name.
6. In the Report Properties window, click the **Output Options** heading to expand the section.
7. Select the **Output to file** check box.
8. In the **Output path** box, update the path of the report to reflect the new name of the Contact Center server.

9. Click **Save Report**.
10. Click **Activate**.
11. Close the report.
12. Repeat step 5 to step 11 for each report.

Variable definitions

Name	Description
Output path	The path of the file in which the historical reports are stored. The path format is \\[computer name]\[shared folder name]\[file name].

Configuring the Contact Center Multimedia settings

About this task

Configure the Contact Center Multimedia configuration settings to ensure that the Multimedia database can find the contacts and has the correct name of the Voice Contact Server.

Procedure

1. Log on to the Voice and Multimedia Contact Server and access the Contact Center Manager Administration Web administration utility.
2. In the Contact Center Manager Administration Web administration utility, click **Multimedia**.
3. In the left column, select the CCMM server name and then click on the **Launch Multimedia Client** button on the right side to launch the CCMM Administration utility.
4. In the CCMM Administration utility, choose **General Administration**.
5. Click **Server Settings**.
6. Select **Contact Center Manager Server**.
7. Click **Edit**.
8. In the **Server Name** box, type the new Voice and Multimedia Contact Server name.
9. Click **Save**.
10. When the warning appears describing potential errors for changing this server, click **OK**.
11. Select **Communication Control Toolkit Server**.
12. Click **Edit**.
13. In the **Server Name** box, type the new Voice and Multimedia Contact Server name.
14. Click **Save**.

15. Select **Contact Center License Server**.
16. Click **Edit**.
17. In the **Server Name** box, type the new Voice and Multimedia Contact Server name.
18. Click **Save**.
19. If you have a backup Contact Center License Manager server, type the name in the **Backup Server** box.
20. Click **Save**.
21. When the warning appears, click **Yes**.
22. Restart the Contact Center Multimedia services. This ensures that Multimedia contacts are routed to agents after changing the Voice and Multimedia Contact Server name.

Updating the HOSTS file for clients

Before you begin

- Determine if you need to update the HOSTS table on your client.

Important:

Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer IP address. This ensures that all clients can interpret the new server name.

Procedure

1. Log on to the client computer.
2. Browse to the HOSTS file in the Windows installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the HOSTS file to reflect the new server name.
5. On the **File** menu, click **Save**.
6. Close all windows.
7. Repeat this procedure on each client computer, so it can communicate with the renamed server.

Configuring the Agent Desktop

Before you begin

- Ensure that agents use the Agent Desktop.
- Change the name of the Voice and Multimedia Contact Server.
- Uninstall the Agent Desktop.

About this task

Configure the Agent Desktop to allow agents to monitor calls and make calls.

Procedure

Install the Agent Desktop.

Important:

Install Agent Desktop using the new server name.

Configuring Avaya Aura® Media Server name resolution

About this task

Configure the Avaya Aura® Media Server hosts file to resolve the hostname and Fully Qualified Domain Name (FQDN) of the Contact Center Manager Administration server. The Contact Center Manager Administration (CCMA) software is installed on the Avaya Aura® Contact Center Voice and Multimedia Contact Server or on the Voice Contact Server.

Procedure

1. Log on to Element Manager with administrative privileges.
2. Navigate to **EM** > **System Configuration** > **Network Settings** > **Name Resolution**.
3. Click **Add**.
4. In the **IP Address** box, enter the Contact Center Manager Administration IP address.
5. In the **Hostname** box, enter the Contact Center Manager Administration hostname.
6. Click **Save**.

Chapter 48: Voice and Multimedia Contact Server IP address change

Change the IP address of the Voice and Multimedia Contact Server where Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, and Contact Center Multimedia are installed on the same server and update the properties of all of the other servers in the Contact Center Suite.

Note:

You can use this chapter to change the IP address of the Voice and Multimedia Contact Server with Avaya Aura® Media Server server.

Changing the contact center subnet IP address of the Voice and Multimedia Contact Server

About this task

You must perform the following steps to update the Voice and Multimedia Contact Server IP address references.

Procedure

1. Log on to the Voice and Multimedia Contact Server.
2. On the **Apps** screen, in the **Avaya** section, select **System Control and Monitor Utility**.
3. On the System Control & Monitor Utility window, click **Shutdown Contact Center**.
4. On the **Start** screen, select **Control Panel**.
5. On the Control Panel screen, click **Network and Internet**.
6. On the Network and Internet screen, click **Network and Sharing Center**.
7. Click **Change adapter settings**.
8. Right-click the LAN connection of the contact center subnet network interface card, and then click **Properties**.
9. Select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
10. Type the new IP address information, and then click **OK**.

11. In the Properties window, click **OK**.

Configuring the Voice and Multimedia Contact Server IP address

About this task

You must perform the following steps to update the Voice and Multimedia Contact Server IP address references.

Procedure

1. Log on to the Voice and Multimedia Contact Server server.
2. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
3. Click the **Local Settings** tab.
4. Under **Avaya Server subnet**, type the new contact center subnet IP address.
5. Click the **Licensing** tab.
6. On the **Updated IP Warning** dialog, click **OK**.
7. Ensure that the **License Server IP** value is the same as the new server IP Address.
8. Click **Apply All**.
9. On the **Restart Required** dialog, click **Yes** to restart the server.

Verifying the server IP address change

About this task

Verify that the Domain Name Service server or network has the correct server IP address.

Procedure

1. Right-click **Start**.
2. Select **Run**.
3. Type `cmd`.
4. Click **OK**.
5. In a Command line window, type `ping <server name>`.

   Where *<server name>* is the name of this server.
6. Verify that the IP address matches the new IP address of the server.

Updating the Network Control Center server

About this task

If your solution uses a Network Control Center (NCC) server, configure it to use the Contact Center Manager Server new IP address.

Note:

If your solution does not use an NCC server, skip this procedure.

Procedure

1. Log on to the Network Control Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Network Configuration**.
3. Click the **Site Table** tab.
4. On the **Site Table** tab, select the site name.
5. Click **Edit**.
6. In the **CLAN IP Address** box, type the new IP address.
7. Click **OK**.
8. On the **Nbconfig** dialog box, click **Verify**.
9. On the **Nbconfig** dialog box, click **OK**.
10. Verify that the correct IP address appears on the **Site Table** tab.
11. Click **OK**.

Updating the HOSTS file

Before you begin

- Determine if you need to update the HOSTS table on your server.

Important:

Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2012 Release 2.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer IP address. This ensures that all servers can interpret the new server name.

Procedure

1. Log on to the server.
2. Browse to the HOSTS file in the Windows Server 2012 Release 2 installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the file to reflect the new server name.
5. On the **File** menu, click **Save**.
6. Close all windows.

Updating the server IP address in CCMA

About this task

You must perform the following steps to update the server IP address references for Contact Center Manager Server in Contact Center Manager Administration.

Procedure

1. On the server, log on to the Contact Center Manager Administration Web administration utility as a user with administrative permissions.
2. Click **Configuration**.
3. Right-click the name of the Contact Center Manager Server.
4. Click **Edit Properties**.
5. In the **IP Address** box, type the new IP address for the server.
6. Click **Submit**.

Updating the HOSTS file for clients

Before you begin

- Determine if you need to update the HOSTS table on your client.

Important:

Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer IP address. This ensures that all clients can interpret the new server name.

Procedure

1. Log on to the client computer.
2. Browse to the HOSTS file in the Windows installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the HOSTS file to reflect the new server name.
5. On the **File** menu, click **Save**.
6. Close all windows.
7. Repeat this procedure on each client computer, so it can communicate with the renamed server.

Updating shared folders for reports

Before you begin

- Ensure that you export scheduled reports in your Contact Center.
- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server (CCMS) name or that you updated the HOSTS file on the clients with the new CCMS name.

Important:

Administrators cannot update the browsers and shared folders for each user, therefore users need to update their respective browsers and shared folders.

About this task

Update the shared folders used for reports to reference the new Contact Center Manager Administration (CCMA) server name in the browser.

Procedure

1. Log on to the server.
2. Log on to the CCMA application as an administrator with all access permissions.
3. Click **Historical Reporting**.
4. In the Historical Reporting main window, on the system tree, click the server under which you want to modify the reports.

5. For each report associated with the new server, click the report name.
6. In the Report Properties window, click the **Output Options** heading to expand the section.
7. Select the **Output to file** check box.
8. In the **Output path** box, update the path of the report to reflect the new name of the Contact Center server.
9. Click **Save Report**.
10. Click **Activate**.
11. Close the report.
12. Repeat step 5 to step 11 for each report.

Variable definitions

Name	Description
Output path	The path of the file in which the historical reports are stored. The path format is \\[computer name]\[shared folder name]\[file name].

Updating the Communication Control Toolkit server IP address in CCMA

About this task

Update the IP address for the Communication Control Toolkit server in Contact Center Manager Administration so you can access Communication Control Toolkit web administration.

Procedure

1. On the server, log on to Contact Center Manager Administration as a user with administrative permissions.
2. Click **Configuration**.
3. Right-click the name of the Communication Control Toolkit Server.
4. Click **Edit Properties**.
5. In the **IP Address** box, type the new server IP address.
6. Click **Submit**.

Verifying the Communication Control Toolkit provider IP address

About this task

Verify that the IP address for the Communication Control Toolkit (CCT) provider in the CCT Web administration utility is the loopback address, so CCT can control voice contacts. If you migrated from an earlier release, the IP address for the CCT provider can be different from the loopback address.

Procedure

1. On the server, add the page: http:\\<*new Server IP Address*> to the list of trusted sites.
2. Log on to Contact Center Manager Administration as a user with administrative permissions.
3. Click **Configuration**.
4. On the left pane, click the name of the Communication Control Toolkit server.
5. Click **Launch CCT Console**.
6. On the **CCT Administration** web administration page, click **Providers**.
7. Click on the provider.
8. In **Basic Provider Information**, in **IP Address**, check that the IP address for the provider is 127.0.0.1.
9. Click **Save**.

Next steps

You must restart CCT using System Control and Monitor Utility (SCMU) if you change the service provider details. On the CCT tab of SCMU, click **Shut down CCT**. When the CCT services are shut down, click **Start CCT**.

Updating the Contact Center Multimedia server IP address in CCMA

About this task

Update the IP address for the Contact Center Multimedia server in Contact Center Manager Administration so you can access Contact Center Multimedia.

Procedure

1. On the server, log on to Contact Center Manager Administration as a user with administrative permissions.
2. Click **Configuration**.

3. Right-click the name of the Contact Center Multimedia Server.
4. Click **Edit Properties**.
5. In the **IP Address** box, type the new server IP address.
6. Click **Submit**.

Configuring Avaya Aura® Media Server name resolution

About this task

Configure the Avaya Aura® Media Server hosts file to resolve the hostname and Fully Qualified Domain Name (FQDN) of the Contact Center Manager Administration server. The Contact Center Manager Administration (CCMA) software is installed on the Avaya Aura® Contact Center Voice and Multimedia Contact Server or on the Voice Contact Server.

Procedure

1. Log on to Element Manager with administrative privileges.
2. Navigate to **EM** > **System Configuration** > **Network Settings** > **Name Resolution**.
3. Click **Add**.
4. In the **IP Address** box, enter the Contact Center Manager Administration IP address.
5. In the **Hostname** box, enter the Contact Center Manager Administration hostname.
6. Click **Save**.

Chapter 49: Voice Contact Server name change

Change the name of the Voice Contact Server where Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit, and other components are installed on the same server and update the properties of all other servers in the Contact Center Suite. The new name of the server must meet the specifications of the server names in the Contact Center suite.

Prerequisites for Voice Contact Server name change

Procedure

- Ensure that the new server name is unique among both the domain and the other servers on the domain.
- Ensure that the new server name is from 6 to 15 characters and that the first character is alphabetical.
- Ensure that the new server name contains no underscores (_), spaces ( ), or punctuation.

Changing the server name in the operating system

About this task

Change the server name on the Voice Contact Server operating system to reflect the new name of the server.

Procedure

1. Log on to the Voice Contact Server as administrator.
2. On the Voice and Multimedia Contact Server, on the **Start** screen, select **Control Panel**.
3. On the Control Panel screen, click **System and Security**.
4. On the System and Security screen, click **System**.
5. In the **Computer name, domain, and workgroup settings** section, click **Change settings**.

6. Click the **Computer Name** tab.
7. Click **Change**.
8. Type the new server name.
9. Click **OK**.
10. When you receive a prompt to restart the server, click **No** to restart later.

    Important:

    Do not restart the server until you synchronize the operating system name with the Voice Contact Server name. See Synchronizing the operating system name with the Voice Contact Server name on page 548.
11. If you are using a Domain Name Service, contact your local network prime to update the DNS with the new server name.

Verifying the server name change

Before you begin

- Ensure that you use a Domain Name Service server in your network.

About this task

Verify that the Domain Name Service server or network has the correct server name.

Procedure

1. Right-click **Start**.
2. Select **Run**.
3. Type `cmd`.
4. Click **OK**.
5. In a Command line window, enter `ping <server name>`.

   Where <*server name*> is the new name of the server.
6. Verify that the IP address matches the IP address of the server with the new name.

Synchronizing the operating system name with the Voice Contact Server name

About this task

Synchronize the operating system name with the Voice Contact Server name to ensure that the Contact Center suite uses the new server name.

Procedure

1. Log on to the Voice Contact Server as administrator.
2. Close the **System Control and Monitor Utility** if it is running.
3. On the **Apps** screen, in the **Avaya** section, select **Computer Update Utility**.
4. Click **OK**.

   If the names do not match, you are prompted to synchronize the names.
5. After the Voice Contact Server services shut down and the synchronize process is complete, click **OK**.
6. On the Synchronization Utility box, click **OK**.
7. Restart the server.

Configuring the server name details

About this task

You must perform the following steps to update the server name references used by Contact Center.

Procedure

1. Log on to the contact center server.
2. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
3. Click the **Local Settings** tab.
4. Verify the server name details.
5. Click **Apply All**.
6. On the **Restart Required** dialog, click **Yes** to restart the server.

Joining the server to the domain

About this task

If you are using a domain and a DNS, you join the Contact Center server to the domain. This ensures that all servers can interpret the new Contact Center server name.

Procedure

1. Log on to the DNS server.
2. On the DNS server, change the server name or IP address of the Contact Center server.
3. Remove the Contact Center server from the domain.
4. Join the Contact Center server back to the domain using the new server name and IP address.

Updating the HOSTS file on the Voice Contact Server

Before you begin

- Determine if you need to update the HOSTS table on your server.

Important:

Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2012 Release 2.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on the Voice Contact Server with the new server name and IP address. This ensures that all servers can interpret the new server name.

Procedure

1. Log on to the Voice Contact Server server.
2. Browse to the HOSTS file in the Windows Server 2012 Release 2 installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the file to reflect the new server name.
5. On the **File** menu, click **Save**.
6. Close all windows.

Resetting the iceAdmin password

Before you begin

- Obtain the domain account name and password from your network administrator, if your Contact Center server is a member of an active domain.

About this task

Contact Center Manager Administration uses the iceAdmin account. Reset the iceAdmin password to access the contents of the Administration database.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Manager Administration Configuration**.
3. In the left pane, click **Avaya**.
4. In the Avaya Applications Configuration window, click **IceAdmin Password Change**.
5. In the **Old Password** box, type the old password.
6. In the **New Password** box, type the new password for the iceAdmin user account.
7. In the **Confirm Password** box, type the password again.

   If your server is a member of an active domain, the Domain Account option is enabled in the iceAdmin Password Change window.
8. To export scheduled reports to a domain network PC, click **Domain Account**.
9. From the **Select Domain Name** list, select the name of the domain to add.
10. In the **Enter Domain Account** box, type the domain account.
11. In the **Enter Domain Account Password** box, type the domain account password.
12. In the **Confirm Domain Account Password** box, type the domain account password again.
13. Click **OK**.
14. Click **OK**.

Configuring destination for exported scheduled reports

Before you begin

- Plan to export scheduled reports to a computer on your domain network.

About this task

If you export scheduled reports to a domain network computer, configure the destination for exported scheduled reports.

Procedure

1. Log on to the server.
2. Create a folder. Name the folder **Exported Reports**.
3. Right-click the new folder and select **Properties**.
4. In the **Properties** dialog box, on the **Sharing** page, click **Advanced Sharing**.
5. Select **Share this folder**.
6. Click **Permissions**.
7. Click **Add**.
8. In the **Select Users or Groups** dialog box, click **Advanced**.

   If Windows Sever 2012 prompts you for an account, enter an account with domain administrative privileges, and enter the account password.
9. Click **Find Now**.
10. In the expanded portion of the **Select Users or Groups** dialog box, locate and select the CCMA administrative account.
11. Click **OK**.
12. In the **Select Users or Groups** dialog box, click **OK**.
13. In the **Permissions** dialog box, select the CCMA administrative account.
14. Select the **Allow** check box for the following:
    - **Change**
    - **Read**
15. Click **Apply**.
16. Click **OK** to close the **Permissions for Exported Reports** dialog box.
17. Click **OK** to close the **Advanced Sharing** dialog box.
18. Click **Close** to close the **Exported Reports Properties** dialog box.

Reconfiguring security certificates after changing the server name

About this task

Re-configure the server security certificates after you change the server name. Complete the following tasks to update the Contact Center security store. For detailed steps on changing the Contact Center security store, see Contact Center security certificates administration on page 447

Procedure

1. Back up the Contact Center security store.
2. Delete the security store.
3. Create a new security store, using the new name of the server.
4. Use the Certificate Signing Request (CSR) from the new store to get a signed server certificate from a Certificate Authority (CA). Alternatively, if you created a new security store and received a certificate before changing the server name, restore that security store. For more information, see Server name change and security certificates on page 521.
5. Import the new signed server certificate and root certificate to the security store.
6. If the CA you used to sign the new server certificate is different to the CA you used to sign the old server certificate, export the new root certificate and distribute it to all the relevant clients and servers.

Changing the server name in the Administration tool

About this task

Change the Contact Center Manager Server name details in the Administration tool to ensure that Contact Center Manager Administration connects to the correct server.

Procedure

1. Log on to the Contact Center Manager Administration application as an administrator with all access permissions.
2. Click **Configuration**.
3. In the left pane, right-click the Contact Center Manager Server name to change.
4. Click **Edit Properties**.
5. Type the new server name, and click **Submit**.

Changing the CCT server name in the Administration tool

About this task

Update the CCT name in the CCMA configuration to ensure that the CCT Web administration launches correctly. Use CCMA to open the CCT Web administration utility.

Procedure

1. Log on to Contact Center Manager Administration.
2. Click **Configuration**.
3. From the **Server** menu, select **CCT Server**.
4. Right-click **CCT Server**, and then click **Edit Properties**.
5. Type the name of the new CCT Server name. Type the new name of this server.

   The system resolves the new CCT server name.
6. Click **Submit**.

Changing the CCMA and CCMM server name in the Dashboard

About this task

Change server names in the CCMM Dashboard to ensure that the CCMM Web administration utility launches.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Multimedia Dashboard**.
3. On the Multimedia Dashboard, under **Server Availability**, right-click **Contact Center Manager Administration** and select **Edit**.
4. On the **Administrator Login** dialog, in the **User Name** box, type `GeneralAdmin`.
5. In the **Password** box, type the password. The default password is "__ccmm!".
6. Click **Login**.
7. On the **Administrator Login** dialog, in the text box, type the name for the current Contact Center Manager Administration server.
8. Click **Save**.
9. On the Multimedia Dashboard, under **Server Availability**, right-click **Contact Center Multimedia Server** and select **Edit**.

10. On the **Administrator Login** dialog, in the **User Name** box, type `GeneralAdmin`.
11. In the **Password** box, type the password. The default password is "__ccmm!".
12. Click **Login**.
13. On the **Administrator Login** dialog, in the text box, type the name for the current Contact Center Multimedia server.
14. Click **Save**.

Updating the HOSTS file for clients

Before you begin

- Determine if you need to update the HOSTS table on your client.

Important:

Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer IP address. This ensures that all clients can interpret the new server name.

Procedure

1. Log on to the client computer.
2. Browse to the HOSTS file in the Windows installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the HOSTS file to reflect the new server name.
5. On the **File** menu, click **Save**.
6. Close all windows.
7. Repeat this procedure on each client computer, so it can communicate with the renamed server.

Updating shared folders for reports

Before you begin

- Ensure that you export scheduled reports in your Contact Center.
- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server (CCMS) name or that you updated the HOSTS file on the clients with the new CCMS name.

Important:

Administrators cannot update the browsers and shared folders for each user, therefore users need to update their respective browsers and shared folders.

About this task

Update the shared folders used for reports to reference the new Contact Center Manager Administration (CCMA) server name in the browser.

Procedure

1. Log on to the server.
2. Log on to the CCMA application as an administrator with all access permissions.
3. Click **Historical Reporting**.
4. In the Historical Reporting main window, on the system tree, click the server under which you want to modify the reports.
5. For each report associated with the new server, click the report name.
6. In the Report Properties window, click the **Output Options** heading to expand the section.
7. Select the **Output to file** check box.
8. In the **Output path** box, update the path of the report to reflect the new name of the Contact Center server.
9. Click **Save Report**.
10. Click **Activate**.
11. Close the report.
12. Repeat step 5 to step 11 for each report.

Variable definitions

Name	Description
Output path	The path of the file in which the historical reports are stored. The path format is \\[computer name]\[shared folder name]\[file name].

Configuring the Contact Center Multimedia settings

Before you begin

- Ensure that the Domain Name Service server is updated with the new Voice Contact Server name. Or update the HOSTS file on the Multimedia Contact Server with the new Voice Contact Server name.

About this task

Configure the Contact Center Multimedia configuration settings to ensure that the Multimedia database can find the contacts and has the correct name of the Voice Contact Server.

Procedure

1. Log on to the Voice Contact Server and access the Contact Center Manager Administration Web administration utility.
2. In the Contact Center Manager Administration Web administration utility, click **Multimedia**.
3. In the left column, select the CCMM server name and then click on the **Launch Multimedia Client** button on the right side to launch the CCMM Administration utility.
4. In the CCMM Administration utility, choose **General Administration**.
5. Click **Server Settings**.
6. Select **Contact Center Manager Server**.
7. Click **Edit**.
8. In the **Server Name** box, type the new Voice Contact Server name.
9. Click **Save**.
10. When the warning appears describing potential errors for changing this server, click **OK**.
11. Select **Communication Control Toolkit Server**.
12. Click **Edit**.
13. In the **Server Name** box, type the new Voice Contact Server name.
14. Click **Save**.
15. When the warning appears describing potential errors for changing this server, click **OK**.
16. Select **Contact Center License Server**.
17. Click **Edit**.
18. In the **Server Name** box, type the new Voice Contact Server name.
19. Click **Save**.
20. If you have a backup Contact Center License Manager server, type the name in the **Backup Server** box.
21. Click **Save**.
22. When the warning appears, click **OK**.

23. Click **Yes** to restart the Contact Center Multimedia services. This ensures that Multimedia contacts are routed to agents after changing the Voice Contact Server name.

Configuring Avaya Aura® Media Server name resolution

About this task

Configure the Avaya Aura® Media Server hosts file to resolve the hostname and Fully Qualified Domain Name (FQDN) of the Contact Center Manager Administration server. The Contact Center Manager Administration (CCMA) software is installed on the Avaya Aura® Contact Center Voice and Multimedia Contact Server or on the Voice Contact Server.

Procedure

1. Log on to Element Manager with administrative privileges.
2. Navigate to **EM** > **System Configuration** > **Network Settings** > **Name Resolution**.
3. Click **Add**.
4. In the **IP Address** box, enter the Contact Center Manager Administration IP address.
5. In the **Hostname** box, enter the Contact Center Manager Administration hostname.
6. Click **Save**.

Chapter 50: Voice Contact Server IP address change

Change the IP address of the Voice Contact Server where Contact Center Manager Server, Contact Center Manager Administration, Communication Control Toolkit are installed on the same server and update the properties of all of the other servers in the Contact Center Suite.

Changing the contact center subnet IP address of the Voice Contact Server

About this task

You must perform the following steps to update the Voice Contact Server IP address references.

Procedure

1. Log on to the Voice Contact Server.
2. On the **Apps** screen, in the **Avaya** section, select **System Control and Monitor Utility**.
3. On the System Control & Monitor Utility window, click **Shutdown Contact Center**.
4. On the **Start** screen, select **Control Panel**.
5. On the Control Panel screen, click **Network and Internet**.
6. On the Network and Internet screen, click **Network and Sharing Center**.
7. Click **Change adapter settings**.
8. Right-click the LAN connection of the contact center subnet network interface card, and then click **Properties**.
9. Select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
10. Type the new IP address, and then click **OK**.
11. In the Properties window, click **OK**.

Configuring the Voice Contact Server IP address

About this task

You must perform the following steps to update the Voice Contact Server IP address references.

Procedure

1. Log on to the Voice Contact Server server.
2. On the **Apps** screen, in the **Avaya** section, select **Server Configuration**.
3. Click the **Local Settings** tab.
4. Under **Avaya Server subnet**, type the new contact center subnet IP address.
5. Click the **Licensing** tab.
6. On the **Updated IP Warning** dialog, click **OK**.
7. Ensure that the Primary Contact Center License Manager IP Address is the same as the new server IP Address.
8. Click **Apply All**.
9. On the **Restart Required** dialog, click **Yes** to restart the server.

Verifying the server IP address change

About this task

Verify that the Domain Name Service server or network has the correct server IP address.

Procedure

1. Right-click **Start**.
2. Select **Run**.
3. Type `cmd`.
4. Click **OK**.
5. In a Command line window, type `ping <server name>`.

   Where <*server name*> is the name of this server.
6. Verify that the IP address matches the new IP address of the server.

Updating the Network Control Center server

About this task

If your solution uses a Network Control Center (NCC) server, configure it to use the Contact Center Manager Server new IP address.

Note:

If your solution does not use an NCC server, skip this procedure.

Procedure

1. Log on to the Network Control Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Network Configuration**.
3. Click the **Site Table** tab.
4. On the **Site Table** tab, select the site name.
5. Click **Edit**.
6. In the **CLAN IP Address** box, type the new IP address.
7. Click **OK**.
8. On the **Nbconfig** dialog box, click **Verify**.
9. On the **Nbconfig** dialog box, click **OK**.
10. Verify that the correct IP address appears on the **Site Table** tab.
11. Click **OK**.

Updating the HOSTS file

Before you begin

- Determine if you need to update the HOSTS table on your server.

Important:

Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2012 Release 2.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer IP address. This ensures that all servers can interpret the new server name.

Procedure

1. Log on to the server.
2. Browse to the HOSTS file in the Windows Server 2012 Release 2 installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the file to reflect the new server name.
5. On the **File** menu, click **Save**.
6. Close all windows.

Updating the server IP address in CCMA

About this task

You must perform the following steps to update the server IP address references for Contact Center Manager Server in Contact Center Manager Administration.

Procedure

1. On the server, log on to the Contact Center Manager Administration Web administration utility as a user with administrative permissions.
2. Click **Configuration**.
3. Right-click the name of the Contact Center Manager Server.
4. Click **Edit Properties**.
5. In the **IP Address** box, type the new IP address for the server.
6. Click **Submit**.

Updating the HOSTS file for clients

Before you begin

- Determine if you need to update the HOSTS table on your client.

Important:

Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer IP address. This ensures that all clients can interpret the new server name.

Procedure

1. Log on to the client computer.
2. Browse to the HOSTS file in the Windows installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the HOSTS file to reflect the new server name.
5. On the **File** menu, click **Save**.
6. Close all windows.
7. Repeat this procedure on each client computer, so it can communicate with the renamed server.

Updating shared folders for reports

Before you begin

- Ensure that you export scheduled reports in your Contact Center.
- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server (CCMS) name or that you updated the HOSTS file on the clients with the new CCMS name.

Important:

Administrators cannot update the browsers and shared folders for each user, therefore users need to update their respective browsers and shared folders.

About this task

Update the shared folders used for reports to reference the new Contact Center Manager Administration (CCMA) server name in the browser.

Procedure

1. Log on to the server.
2. Log on to the CCMA application as an administrator with all access permissions.
3. Click **Historical Reporting**.
4. In the Historical Reporting main window, on the system tree, click the server under which you want to modify the reports.

5. For each report associated with the new server, click the report name.
6. In the Report Properties window, click the **Output Options** heading to expand the section.
7. Select the **Output to file** check box.
8. In the **Output path** box, update the path of the report to reflect the new name of the Contact Center server.
9. Click **Save Report**.
10. Click **Activate**.
11. Close the report.
12. Repeat step 5 to step 11 for each report.

Variable definitions

Name	Description
Output path	The path of the file in which the historical reports are stored. The path format is \\[computer name]\[shared folder name]\[file name].

Updating the Communication Control Toolkit server IP address in CCMA

About this task

Update the IP address for the Communication Control Toolkit server in Contact Center Manager Administration so you can access Communication Control Toolkit web administration.

Procedure

1. On the server, log on to Contact Center Manager Administration as a user with administrative permissions.
2. Click **Configuration**.
3. Right-click the name of the Communication Control Toolkit Server.
4. Click **Edit Properties**.
5. In the **IP Address** box, type the new server IP address.
6. Click **Submit**.

Verifying the Communication Control Toolkit provider IP address

About this task

Verify that the IP address for the Communication Control Toolkit (CCT) provider in the CCT Web administration utility is the loopback address, so CCT can control voice contacts. If you migrated from an earlier release, the IP address for the CCT provider can be different from the loopback address.

Procedure

1. On the server, add the page: http:\\<*new Server IP Address*> to the list of trusted sites.
2. Log on to Contact Center Manager Administration as a user with administrative permissions.
3. Click **Configuration**.
4. On the left pane, click the name of the Communication Control Toolkit server.
5. Click **Launch CCT Console**.
6. On the **CCT Administration** web administration page, click **Providers**.
7. Click on the provider.
8. In **Basic Provider Information**, in **IP Address**, check that the IP address for the provider is 127.0.0.1.
9. Click **Save**.

Next steps

You must restart CCT using System Control and Monitor Utility (SCMU) if you change the service provider details. On the CCT tab of SCMU, click **Shut down CCT**. When the CCT services are shut down, click **Start CCT**.

Configuring Avaya Aura® Media Server name resolution

About this task

Configure the Avaya Aura® Media Server hosts file to resolve the hostname and Fully Qualified Domain Name (FQDN) of the Contact Center Manager Administration server. The Contact Center Manager Administration (CCMA) software is installed on the Avaya Aura® Contact Center Voice and Multimedia Contact Server or on the Voice Contact Server.

Procedure

1. Log on to Element Manager with administrative privileges.
2. Navigate to **EM** > **System Configuration** > **Network Settings** > **Name Resolution**.

3. Click **Add**.
4. In the **IP Address** box, enter the Contact Center Manager Administration IP address.
5. In the **Hostname** box, enter the Contact Center Manager Administration hostname.
6. Click **Save**.

Chapter 51: Multimedia Contact Server name change

Change the name of the Multimedia Contact Server and update the properties of all other servers in the Contact Center Suite. The new name of the server must meet the specifications of the server names in the Contact Center suite.

Prerequisites for Multimedia Contact Server name change

Procedure

- Ensure that the new server name is unique among both the domain and the other servers on the domain.
- Ensure that the new server name is from 6 to 15 characters in which the first character is alphabetical.
- Ensure that the new server name contains no underscores (_), spaces ( ), or punctuation.

Turning off Web Services security

About this task

Turn off Web Services security before you rename the server. If Web Services security is not enabled on your contact center, you can skip this procedure.

Procedure

1. Log on to the Contact Center server as a local administrator.

   Important:

   If you log on to the server as a domain administrator, this procedure does not complete successfully.

2. On the **Apps** screen, in the **Avaya** section, select **Security Manager**.
3. On the Store Access dialog, type the password for the security store, and click **OK**.
4. On the Security Manager screen, select the **Security Configuration** tab.

5. Click **Security Off**.
6. Click **Apply**.
7. On the Security Change Confirmation dialog, click **Confirm**.
8. Click **Log Out**.
9. Restart the Contact Center server.

Changing the server name on the operating system

About this task

Change the Multimedia Contact Server name on the operating system so that the server software recognizes the new name in the Contact Center.

Procedure

1. Log on to the Multimedia Contact Server server.
2. On the Voice and Multimedia Contact Server, on the **Start** screen, select **Control Panel**.
3. On the Control Panel screen, click **System and Security**.
4. On the System and Security screen, click **System**.
5. In the **Computer name, domain, and workgroup settings** section, click **Change settings**.
6. Click the **Computer Name** tab.
7. Click **Change**.
8. Enter the new server name.
9. Click **OK**.
10. When you receive a prompt to restart the server, click **No** to restart later.

    Important:

    Do not restart the server until you synchronize the operating system name with the Multimedia Contact Server name. See Synchronizing the operating system name with the Multimedia Contact Server name on page 568.
11. If you are using a Domain Name Service, contact your local network prime to update the DNS with the new server name.

Verifying the server name change

Before you begin

- Ensure that you use a Domain Name Service server in your network.

About this task

Verify that the Domain Name Service server or network has the correct server name.

Procedure

1. Right-click **Start**.
2. Select **Run**.
3. Type `cmd`.
4. Click **OK**.
5. In a Command line window, enter `ping <server name>`.

   Where <*server name*> is the new name of the server.
6. Verify that the IP address matches the IP address of the server with the new name.

Synchronizing the operating system name with the Multimedia Contact Server name

About this task

Synchronize the operating system name with the Multimedia Contact Server name to ensure that the Contact Center suite uses the new server name.

Procedure

1. Log on to the Multimedia Contact Server as administrator.
2. Close the **System Control and Monitor Utility** if it is running.
3. On the **Apps** screen, in the **Avaya** section, select **Computer Update Utility**.
4. Click **OK**.

   If the names do not match, you are prompted to synchronize the names.
5. After the Contact Center Multimedia services shut down and the synchronize process is complete, click **OK**.
6. On the **Synchronisation Utility** box, click **OK**.
7. Restart the server.

Joining the server to the domain

About this task

If you are using a domain and a DNS, you join the Contact Center server to the domain. This ensures that all servers can interpret the new Contact Center server name.

Procedure

1. Log on to the DNS server.
2. On the DNS server, change the server name or IP address of the Contact Center server.
3. Remove the Contact Center server from the domain.
4. Join the Contact Center server back to the domain using the new server name and IP address.

Updating the HOSTS file on the Multimedia Contact Server

Before you begin

- Determine if you need to update the HOSTS table on your server.

Important:

Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2012 Release 2.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on the Multimedia Contact Server with the new server name and IP address. This ensures that all servers can interpret the new server name.

Procedure

1. Log on to the Multimedia Contact Server server.
2. Browse to the HOSTS file in the Windows Server 2012 Release 2 installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the file to reflect the new server name.
5. On the **File** menu, click **Save**.
6. Close all windows.

Reconfiguring security certificates after changing the server name

About this task

Re-configure the server security certificates after you change the server name. Complete the following tasks to update the Contact Center security store. For detailed steps on changing the Contact Center security store, see Contact Center security certificates administration on page 447

Procedure

1. Back up the Contact Center security store.
2. Delete the security store.
3. Create a new security store, using the new name of the server.
4. Use the Certificate Signing Request (CSR) from the new store to get a signed server certificate from a Certificate Authority (CA). Alternatively, if you created a new security store and received a certificate before changing the server name, restore that security store. For more information, see Server name change and security certificates on page 521.
5. Import the new signed server certificate and root certificate to the security store.
6. If the CA you used to sign the new server certificate is different to the CA you used to sign the old server certificate, export the new root certificate and distribute it to all the relevant clients and servers.

Changing the CCMA and CCMM server name in the Dashboard

About this task

Change server names in the CCMM Dashboard to ensure that the CCMM Web administration utility launches.

Procedure

1. Log on to the Contact Center server.
2. On the **Apps** screen, in the **Avaya** section, select **Multimedia Dashboard**.
3. On the Multimedia Dashboard, under **Server Availability**, right-click **Contact Center Manager Administration** and select **Edit**.
4. On the **Administrator Login** dialog, in the **User Name** box, type `GeneralAdmin`.
5. In the **Password** box, type the password. The default password is "__ccmm!".
6. Click **Login**.

7. On the **Administrator Login** dialog, in the text box, type the name for the current Contact Center Manager Administration server.
8. Click **Save**.
9. On the Multimedia Dashboard, under **Server Availability**, right-click **Contact Center Multimedia Server** and select **Edit**.
10. On the **Administrator Login** dialog, in the **User Name** box, type `GeneralAdmin`.
11. In the **Password** box, type the password. The default password is "__ccmm!".
12. Click **Login**.
13. On the **Administrator Login** dialog, in the text box, type the name for the current Contact Center Multimedia server.
14. Click **Save**.

Updating the email attachment folders

Before you begin

- Ensure that you have the email feature installed and enabled using the Contact Center License Manager.

About this task

Update the email attachment folders for Contact Center Multimedia. If you are licensed for email messages in your contact center, you must update the email attachment folders.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, from the **CCMM Servers** list, select your CCMM server.
3. Click **Launch Multimedia Client**.

   The CCMM Administration utility opens.
4. In the left column of the CCMM Administration utility, select **E-mail**.
5. Select **General Settings**.
6. In the **Attachment Files** area, update the path to match the new server path.
7. Click **Save**.

Changing the server name for Enterprise Web Chat

About this task

If your contact center implements Avaya Enterprise Web Chat, update the CCMM server name for EWC.

Before you begin

Shut down the CCMM services using SCMU.

Procedure

1. Log on to the Multimedia Contact Server
2. Right-click **Start**.
3. Select **Run**.
4. Type `cmd`.
5. Click **OK**.
6. In the command line window, enter `CD D:\Avaya\Contact Center \EnterpriseWebChat\eJabberd`
7. Enter `update_hostname.bat <CCMM_servername>`

   where <CCMM_servername> is the new Multimedia Contact Server name.
8. Use SCMU to start the CCMM services.

Configuring the external Web Communications server

Before you begin

- Know the custom interface folder names and paths for the web.xml and .jsp files for the sample Web communications installation.

About this task

If your solution uses an external Web Communications server, configure the Web Communications server to update the files with the new server name.

You must update for .jsp files with Apache Tomcat. If you use a different servlet engine (for example, JRun or WebLogic) or a different technology (ASP.NET), you must use the standard procedures for your environment.

Procedure

1. Log on to your external Web Communications Web server.
2. Open the config file located at `C:\xampp\htdocs\Code\include` in Notepad or another text editor.

3. Locate the text string CCMM_MACHINE_NAME and update the new server name after the '=' sign.
4. Save and close the file.

Updating the CCMM server information in Contact Center Manager Administration

Before you begin

- Change the name of the Contact Center Multimedia server. Changing the server name on the operating system on page 567.

About this task

Update the Contact Center Multimedia server name in the Contact Center Manager Administration to ensure that CCMM launches correctly. You can configure more than one Contact Center Multimedia server in Contact Center Manager Administration, but only one Contact Center Multimedia server is active at a time.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. In a Web browser, start the Contact Center Manager Administration browser.
3. Click **Configuration**.
4. From the **Server** menu, select **CCMM Server**.
5. Right-click **CCMM Server** and then click on **Edit Properties**.
6. Type the name of the new CCMM server.

   The system automatically resolves the IP address and displays the name.
7. In the **Password** box, retype the password for the reporting user name for the server.
8. Click **Submit**.

Variable definitions

Name	Description
CCMA_ServerName	The name of the server where Contact Center Manager Administration is installed.
Login ID	The name used to generate multimedia reports. The default logon ID for the Contact Center Multimedia server is mmReport.

Table continues…

Name	Description
Password	The password used for the ID used to generate multimedia reports. The default user password is mmRep.

Updating the HOSTS file for clients

Before you begin

- Determine if you need to update the HOSTS table on your client.

Important:

Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer IP address. This ensures that all clients can interpret the new server name.

Procedure

1. Log on to the client computer.
2. Browse to the HOSTS file in the Windows installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the HOSTS file to reflect the new server name.
5. On the **File** menu, click **Save**.
6. Close all windows.
7. Repeat this procedure on each client computer, so it can communicate with the renamed server.

Configuring the Agent Desktop

Before you begin

- Ensure that agents use the Agent Desktop.
- Change the name of the Multimedia Contact Server.

- Uninstall the Agent Desktop.

About this task

Configure the Agent Desktop to allow agents to monitor calls and make calls.

Procedure

Install the Agent Desktop.

Important:

Install Agent Desktop using the new server name.

Chapter 52: Multimedia Contact Server IP address change

Change the IP address of the Multimedia Contact Server and update the properties of all of the other servers in the Contact Center Suite.

Changing the IP address on the operating system

Before you begin

- Know how to stop and restart the Contact Center Multimedia services.

About this task

Change the Contact Center Multimedia server IP address on the operating system to ensure that the server has the correct information and other servers in Contact Center can locate it.

Procedure

1. Log on to the Contact Center Multimedia server.
2. Stop all of the multimedia services.
3. On the **Start** screen, select **Control Panel**.
4. On the Control Panel screen, click **Network and Internet**.
5. On the Network and Internet screen, click **Network and Sharing Center**.
6. Click **Change adapter settings**.
7. Right-click the LAN connection, and then click **Properties**.
8. Select **Internet Protocol (TCP/IP)**, and then click **Properties**.
9. In the **IP Address** box, type the new IP address.
10. Click **OK**.
11. On the Properties window, click **Close**.
12. Restart the multimedia services.

Verifying the server IP address change

About this task

Verify that the Domain Name Service server or network has the correct server IP address.

Procedure

1. Right-click **Start**.
2. Select **Run**.
3. Type `cmd`.
4. Click **OK**.
5. In a Command line window, type `ping <server name>`.

   Where *<server name>* is the name of this server.
6. Verify that the IP address matches the new IP address of the server.

Updating the HOSTS file

Before you begin

- Determine if you need to update the HOSTS table on your server.

Important:

Incorrectly modifying a host table can cause extensive network problems. Before you modify host tables, review the information about hosts in the supporting documentation for Microsoft Windows Server 2012 Release 2.

About this task

If you do not have a DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer IP address. This ensures that all servers can interpret the new server name.

Procedure

1. Log on to the server.
2. Browse to the HOSTS file in the Windows Server 2012 Release 2 installation directory, `C:\Windows\system32\drivers\etc`.
3. Right-click the HOSTS file and open the file with a text editor such as Notepad to modify the host tables.
4. Update the file to reflect the new server name.
5. On the **File** menu, click **Save**.
6. Close all windows.

Updating the CCMM server IP address in Contact Center Manager Administration

Before you begin

- Change the IP address of the Contact Center Multimedia server. Changing the IP address on the operating system on page 576.

About this task

Update the Contact Center Multimedia server IP address in the Contact Center Manager Administration to ensure that CCMM launches correctly.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. In a Web browser, start the Contact Center Manager Administration browser.
3. Click **Configuration**.
4. From the **Server** menu, select **CCMM Server**.
5. Right-click **CCMM Server** and then click on **Edit Properties**.
6. In the **IP Address** box, type the new server IP address.
7. In the **Password** box, retype the password for the reporting user name for the server.
8. Click **Submit**.

Variable definitions

Name	Description
CCMA_ServerName	The name of the server where Contact Center Manager Administration is installed.
Login ID	The name used to generate multimedia reports. The default logon ID for the Contact Center Multimedia server is mmReport.
Password	The password used for the ID used to generate multimedia reports. The default user password is mmRep.

Chapter 53: Avaya Aura® Media Server server name change

Change the name of the Avaya Aura® Media Server server and update the properties of all of the other servers in the Avaya Aura® Contact Center suite.

Note:

You can use this chapter to change the name of the Avaya Aura® Media Server Hyper-V instance.

Changing the name of the Avaya Aura® Media Server on Linux

Before you begin

- Stop Avaya Aura® Contact Center using System Control and Monitor Utility (SCMU) or System Management and Monitoring Component (SMMC).

About this task

Perform the following procedure if you need to change the host name of a Linux based Avaya Aura® Media Server.

Procedure

1. Access the Element Manager (EM) of the server.
2. Navigate to **EM** > **System Status** > **Element Status**.
3. Click **Stop**.
4. Click **Confirm** to proceed with the action.

   After a few seconds, the system updates the status fields and activates or deactivates the buttons based on the new state of the media server.
5. On the Linux server, edit the file `/etc/hosts`.
6. Update the host name wherever the host name appears in the file.
7. Save the file.

8. Edit the file `/etc/sysconfig/network`.
9. Update the host name wherever the host name appears in the file.
10. Save the file.
11. Using a Linux shell, enter the following command to apply the host name change to the system:

    ```
    hostname <new_hostname>
    ```

    Where <new_hostname> is the new name for the server.
12. If this server is a member of a cluster or High Availability pair, then navigate to **EM** > **Cluster Configuration** > **Server Designation** on each server and ensure the server details you just changed are updated on each server.
13. Navigate to **EM** > **System Status** > **Element Status**.
14. Click **Start**.
15. Click **Confirm** to proceed with the action.

Re-configuring security certificates after changing the Avaya Aura® Media Server server name

About this task

Re-configure the server security certificates after you change the server name. Complete the following tasks to update the Avaya Aura® Media Server security store. For detailed steps on changing the certificates, see Avaya Aura Media Server security certificates administration on page 476.

Procedure

1. Create a new CSR for Avaya Aura® Media Server, using the new name of the server.
2. Use the new CSR to get a signed server certificate from a Certificate Authority (CA) for Avaya Aura® Media Server.
3. If the CA you used to sign the new Avaya Aura® Media Server server certificate is different to the CA you used to sign the old server certificate, export the new root certificate and distribute it to all the relevant clients and servers.

Updating the standalone Avaya Aura® Media Server name in CCMA

About this task

Update the media server details configured in Contact Center Manager Administration to match the new Avaya Aura® Media Server server name.

Procedure

1. Log on to Contact Center Manager Administration with administrator privileges.
2. On the **Launchpad**, click **Configuration**.
3. In the left pane, click the plus (+) sign next to the SIP-enabled Contact Center Manager Server.
4. From the list of configuration items for the Contact Center Manager Server, select **Media Servers**.
5. On the **Media Servers** window, in the **Server Name** box, type the name of the Avaya Aura® Media Server server.
6. Click any other cell in the table to save your changes.
7. Repeat step 5 to step 6 for each media server to update.

Chapter 54: Avaya Aura® Media Server IP address change

Change the IP address of the Avaya Aura® Media Server and update the properties of all of the other servers in the Avaya Aura® Contact Center suite.

Note:

You can use this chapter to change the IP address of the Avaya Aura® Media Server Hyper-V instance.

Changing the Avaya Aura® Media Server IP address on Linux

Before you begin

- Stop Avaya Aura® Contact Center using System Control and Monitor Utility (SCMU) or System Management and Monitoring Component (SMMC).

About this task

Stop Avaya Aura® Media Server before changing the IP address. Perform the following procedure if you need to change the IP address of a Linux based Avaya Aura® Media Server. The network adapter names and network configuration file names can be different on your server.

Procedure

1. Access the Element Manager (EM) of the server.
2. Navigate to **EM** > **System Status** > **Element Status**.
3. Click **Stop**.
4. Click **Confirm** to proceed with the action.

   After a few seconds, the system updates the status fields and activates or deactivates the buttons based on the new state of the media server.
5. On the Linux server, edit the file `/etc/hosts`.
6. Update the IP Address wherever it appears in the file.
7. Save the file.

8. Edit the file `/etc/sysconfig/network-scripts/ifcfg-eth0`.
9. Update the IP address wherever the IP address appears in the file.
10. Save the file.
11. Using the local Linux console shell, enter the following commands to apply the IP address change to the system:

    ```
    /etc/init.d/network stop
    ```

    ```
    /etc/init.d/network start
    ```

12. Login to EM using the new IP address in the URL for the EM login.
13. Navigate to **EM** > **System Configuration** > **Network Settings** > **IP Interface Assignment**.
14. **IP Interface Assignment** fields show errors, as a result of the IP address change. Select valid IP addresses from the drop-down menus for each field showing **Invalid**.
15. Click **Save**.
16. Click **Confirm**.
17. Using the local Linux console shell, enter the following commands to restart Avaya Aura® Media Server:

    ```
    reboot
    ```

18. If this server is a member of a cluster or High Availability pair, then navigate to **EM** > **Cluster Configuration** > **Server Designation** on each server and ensure the IP address you just changed is updated on each server.
19. Restart the server.

Updating the standalone Avaya Aura® Media Server IP address in CCMA

About this task

Update the media server details configured in Contact Center Manager Administration to match the new Avaya Aura® Media Server IP address.

Procedure

1. Log on to Contact Center Manager Administration with administrator privileges.
2. On the **Launchpad**, click **Configuration**.
3. In the left pane, click the plus (+) sign next to the SIP-enabled Contact Center Manager Server.

4. From the list of configuration items for the Contact Center Manager Server, select **Media Servers**.
5. In the **IP Address** box, type the IP address of the Avaya Aura® Media Server.
6. Click any other cell in the table to save your change.
7. Repeat step 5 to step 6 for each media server to update.

Appendix A: Default login values

You can log on to the different Contact Center applications with the default login values listed in the following table. Refer to the list to acquire the default usernames and passwords.

Application	Default user ID	Default Password	Notes
Manager Server – Commissioning	Administrator	<user defined>	
Server Administration – Server Utility	sysadmin	avaya1	
Manager Administration Commissioning – iceAdmin user ID	<user sets up their own account>	<user sets up their own account>	
Manager Administration	webadmin	webadmin	
Manager Administration – Commissioning	sysadmin	avaya1	
Virtual directories for IIS – Commissioning	<servername> \CCMMOPSUSER	_mm6NtRed!	
CCT clients	Windows user configured in CCT client		Failed authentication attempts are not logged in the NCCT Security Log because Windows only invokes the CCT service after successfully authenticating the client credentials.
Process Monitor – Common Utilities		__avaya (underscore, underscore, a, v, a, y, a)	
Trace Control Utility – Common Utilities		__avaya (underscore, underscore, a, v, a, y, a)	

Index

A

AAEP 51
access class
create 93
delete 96
modify 94
access classes
add 175
operations 92
view members 94
access classes operations
create access class 93
delete access class 96
log on to Server Utility 92
modify access class 94
preview list of access classes 95
print list of access classes 96
view members of access classes 94
Access database 418
access to email message text
control 364
activate offline store 459
active callback timer
configure 368
active callback trunk access
configure 369
active contact timer
configure 368
add
access classes 175
administrators 226
desktop user accounts 103
document imaging server 300
email server 245
event preference 115
expert manually to CCMM 328
experts to a skillset 330
fax mailbox 312
fax server 310
network skillset 181
scanned document mailbox 302
site in CCMS 175
site to the NCC 172
SMS Gateway 333
SMS mailbox 335
specified length to all voice segments 130
voice mail mailbox 293
voice mail server 291
add administrator email address
CCMM Dashboard 283
add event preference
variable definitions 116
add fax mailbox
variable definitions 312
adding friendly name 363
add scanned document mailbox
variable definitions 303
add SMS mailbox
variable definitions 335
add voice mail mailbox
variable definitions 294
administer
connected user and user account operations 97
administration
console 191
licensing 85
NCC server 172
SNMP 486
administrators
add 226
remove 228
advanced application
configure 380
advanced filters
configure 381
advanced screen pops
configure 382
agent
supervisor approval for email messages 365
Whisper Coaching 33
agent access to contacts
configure 365
Agent Desktop
configure 363
disabling embedded softphone 366
force password complexity for Multimedia accounts 31
integration with Enterprise Web Chat 28
process email contacts 212
process email contact types 218
process outbound contacts 219
Agent Desktop Advanced Settings
configure 387
Agent Desktop behavior
Bring to front 370
configure 370
Give focus 370
Agent Desktop configuration
change a closed reason 373
change custom fields in Agent Desktop 367
configure active contact timer 368
configure advanced applications 380
configure advanced filters 381
configure advanced screen pops 382
configure Advanced Settings 387
configure Advanced Settings in a voice-only solution 391

configure state of the Agent terminal *(continued)*
configure agent access to contacts ... 365
configure Agent Desktop behavior ... 370
configure basic screen pops ... 376
configure callback timer ... 368
configure callback trunk access ... 369
configure default closed reasons ... 374
configure hotdesking
Citrix environment ... 372
configure state of the Agent terminal
log off ... 371
configure Web reporting ... 373
configure Web statistics ... 372
control access to email message text ... 364
create a closed reason ... 373
create custom fields in Agent Desktop ... 367
delete closed reason ... 375
delete custom field in Agent Desktop ... 367
enable customer history on voice contacts ... 385
shortcut keys ... 375
specify email attachment size ... 370
Agent Desktop Displays parameters on the server
configure ... 145
variable definitions ... 146
Agent Order Preference
configure ... 183
agent-supervisor barge-in
configure intrinsics ... 361
agent-supervisor observe
configure intrinsics ... 361
agent timers
configure ... 348
alarm
configure ... 112
Alarm Monitor
manually clear an alarm ... 121
obtain more information about alarms ... 120
open ... 118
refresh ... 119
sort events ... 119
Alarm Monitor appears in the foreground
procedure job aid ... 120
alias for a recipient mailbox
change ... 250
create ... 250
all silence from all voice segments
remove ... 131
application commands
HAI service functionality ... 40
SEND INFO ... 41
SEND REQUEST and GET RESPONSE ... 40
apply
office hours ... 230
archive rule ... 420
archive scheduled task ... 420
assign
development Web server name ... 343
assign a development Web server name
variable definitions ... 344
automatic phrases (IM)
create ... 327
automatic phrases (Web communications)
create ... 351
delete ... 352
auto-rejection of email messages
keyword groups ... 273
Avaya Aura Media Server
configuration ... 436
Avaya Aura Media Server security ... 476
Avaya Aura MS
root certificate ... 476
Avaya CRQM
configure ... 151
Avaya Media Server ... 34
Avaya WebLM ... 89

B

backing up security store ... 449
Barge-in and Observation tone ... 34
barred email address
delete ... 278
barring
outgoing email address ... 277
basic screen pops
configure ... 376
bulk resources
export ... 200
import ... 199

C

Call Force Answer Zip Tone ... 34
CallPilot ... 51
capture
CDN data ... 161
IVR ACD-DN data ... 162
route data ... 163
TN data ... 159
voice port data ... 161
capturing terminal data
example ... 160
CCMA
configure ... 134
CCMA configuration
configure Agent Desktop Displays parameters on the server ... 145
configure Avaya CRQM ... 151
configure CDN Landing Pads for Integrated Reporting ... 152
configure CDN Landing Pads for Universal Networking ... 152
configure DNIS Landing Pads for Universal Networking ... 153

CCMA configuration *(continued)*
configure email notifications (Historical reporting) 139
configure Emergency Help 138
configure logon warning message title and text 134
configure LPR port for printers 149
configure network printer 149
configure Real-Time Reporting 136
configure security settings 143
configure SMTP server 140
create shared folder to export historical reports 142
enable logon warning message 135
install Orchestration Designer 144
install XML Automated Assignments feature 150
prerequisites 134
CCMM
fundamentals 204
general configuration 224
CCMM Dashboard 215
add administrator email address 283
CCMM fundamentals
email contact type 205
email traffic reports 208
fax 216
instant Messaging 221
mailbox configuration 217
office hours 221
outbound contact type 218
scanned documents 216
SMS 216
traffic reports 217
voice mail 216
voice-only solution 222
Web communications 220
CCMM general configuration
add administrators 226
apply office hours 230
configure Directory LDAP server 237
configure displayed date for traffic reports 232
configure geographic alternate CCT server 235
configure holidays 229
configure office hours 228
configure reporting credentials 226
configure system license 225
configure Web communications comfort groups
WC skillset 234
configure Web On Hold comfort groups
WC skillset 232
delete geographic alternate CCT server 236
prerequisites 224
remove administrators 228
remove Web communications comfort groups
WC skillset 234
remove Web On Hold comfort groups
WC skillset 233
view
real-time traffic reports by contact 231
CCMM server IP address change
CCMM server IP address change *(continued)*
change the IP address on the operating system 576
update the CCMM server IP address in CCMA 578
CCMM server name change
configure the external Web server
Web communications 533, 572
dashboard 532, 553, 570
update CCMM server information in CCMA 573
update email attachment folders 533, 571
CCMS
configuration 46
CS 1000 switch data 50
feature report 43
host application integration service functionality 38
licensed features configuration 48
local settings configuration 47
Multicast Address and Port Configuration 43
Multicast Stream Control 43
Nbconfig 44
real-time statistics
manual 43
server configuration 44
server settings 110
SIP Local Subscriber data 52
SIP Network Settings data 54
web services 45
CCMS configuration
prerequisites 46
CCMS connected user operations
prerequisites 97
CCMS flow application
configure 77
CCMS Network Configuration utility
regular access level 46
CCMS Serial port
configure
prerequisites 108
CCMS server settings
prerequisites 110
view server resources 110
CCMS statistics
configuration 57
CCMS statistics configuration
change IP multicast settings 59
configure Multicast controller 57
disconnect Terminal Services sessions 60
prerequisites 57
CCMS Utility
access classes operations
prerequisites 92
view CCMS events 445
CCSA 34
CCT
fundamentals 191
Open Interfaces 193
Reference Client 193
Web Administration 192

CCT fundamentals
ACD ... 191
administration console ... 191
application programming interfaces ... 192
CCT Reference Client ... 193
CCT Web Administration ... 192
programming interfaces ... 192
Trace Control Utility ... 192
Web services ... 193
CDN data
capture ... 161
CDN Landing Pads for Integrated Reporting
configure ... 152
CDN Landing Pads for Universal Networking
configure ... 152
change
alias for a recipient mailbox ... 250
character encoding for outgoing email ... 275
closed reason ... 373
CS 1000 switch data ... 50
custom fields in Agent Desktop ... 367
event classification ... 118
event preference ... 117
filtering criteria for events ... 114
IP address ... 521
IP multicast settings ... 59
keyword group ... 256
licensed features configuration ... 48
license manager file on CCMS ... 88
Multimedia Contact Server IP address ... 576
Multimedia Contact Server name ... 566
Nodal to Corporate licensing ... 87
prepared responses ... 258
properties of desktop users ... 106
recipient mailbox ... 247
rule groups ... 270
rules ... 265
sender group ... 263
sequence of messages
Web communications comfort groups ... 359
server name ... 521
SIP Local Subscriber data ... 52
SIP Network Settings data ... 54
Voice and Multimedia Contact Server IP address ... 538
Voice and Multimedia Contact Server server name ... 524
Voice Contact Server IP address ... 558
Voice Contact Server server name ... 546
change CS 1000 switch data
variable definitions ... 51
Change IP address ... 581, 583
change IP multicast settings
procedure job aid ... 60
variable definitions ... 60
change licensed features configuration
variable definitions ... 49
change local settings configuration
variable definitions ... 47
change SIP Local Subscriber data
variable definitions ... 53
change SIP Network Settings data
variable definitions ... 54
change the CCMM server name
Administration tool ... 532
CCMA ... 532
change the CCT server name
Administration tool ... 531, 553
CCMA ... 531, 553
changing
IP address on Linux ... 582
local settings configuration ... 47
character encoding
outgoing email messages ... 207
cleanup rule
closed reason ... 427
customer ... 428
email rules ... 426
outbound campaign ... 425
skillset ... 426
cleanup scheduled task
creating ... 429
client browsers and shared folders
update ... 534, 542, 555, 562
closed reason
change ... 373
cleanup rule ... 427
create ... 373
delete ... 375
compatibility
language family ... 166
concurrently running one-X Communicator with Agent Desktop ... 28
configure
active callback timer ... 368
active callback trunk access ... 369
active contact timer ... 368
advanced applications ... 380
advanced filters ... 381
advanced screen pops ... 382
agent access to contacts ... 365
Agent Desktop ... 363
Agent Desktop Advanced Settings ... 387, 391
Agent Desktop behavior ... 370
Agent Desktop Displays parameters on the server ... 145
Agent Order Preference ... 183
agent timers ... 348
alarm ... 112
Avaya CRQM ... 151
basic screen pops ... 376
CCMA ... 134
CCMS ... 46
CCMS flow application ... 77
CCMS statistics ... 57
CDN Landing Pads for Integrated Reporting ... 152
CDN Landing Pads for Universal Networking ... 152

Web On Hold comfort groups *(continued)*
CS 100 PABX ... 111
customer notification log ... 350
database connections ... 66
Database Integration Wizard ... 62
data source name ... 63
default closed reasons ... 374
Directory LDAP server ... 237
disconnect messages ... 326
displayed date for traffic reports ... 232
DNIS Landing Pads for Universal Networking ... 153
DNIS network CDNs ... 188
email ... 242
email notifications (Historical reporting) ... 139
email server names ... 243
email settings ... 274
Emergency Help ... 138
event ... 112
external Web server
Web communications ... 533, 572
fax ... 309
fax reply mailbox ... 314
geographic alternate CCT server ... 235
HDX provider ID ... 64
historical statistics collection ... 186
holidays ... 229
hotdesking
Citrix environment ... 372
hot-standby automatic switchovers ... 499
hot-standby managed IP address ... 492
hot standby manual switchovers ... 496
hot-standby server ... 493
instant message ... 326
log filter settings ... 440
logon warning message title and text ... 134
LPR port for printers ... 149
mailbox ... 217
MCDN network CDNs ... 187
Microsoft Exchange for sending outgoing email ... 278
Mission Critical High Availability ... 501
Mission Critical High Availability on the standby server ... 503
mmReport user ... 226
Multicast controller ... 57
Multimedia server settings ... 535, 556
network communication parameters ... 178
network skillset properties ... 182
NMS ... 490
notification of automatic switchovers ... 495
office hours ... 228
Open Interfaces for email ... 285
outbound ... 240
Real-Time Reporting ... 136
reporting credentials ... 226
route point
fax skillset ... 309
scanned document skillset ... 300
Web On Hold comfort groups *(continued)*
route point for an SMS skillset ... 333
route point for a voice mail skillset ... 291
routing table assignments ... 184
routing tables ... 184
scanned document ... 299
scanned document reply mailbox ... 304
security settings ... 143
Serial port ... 108
service monitoring ... 497
shortcut keys ... 375
skillsets for email ... 247
SMS ... 332
SMS reply mailbox ... 337
SMTP server on CCMA server ... 140
SN system default rule ... 320
Social Networking channels ... 321
Social Networking languages ... 321
Social Networking mailboxes ... 322
state of the Agent terminal
log off ... 371
system license ... 225
TAPI server settings ... 65
voice mail ... 290
Voice Prompt Editor ... 122
Web communications ... 342
Web communications comfort groups
WC skillset ... 234
Web On Hold comfort groups
WC skillset ... 232
Web services ... 67
welcome messages ... 326, 344
configure Agent Desktop Advanced Settings
variable definitions ... 387
configure Agent Desktop Advanced Settings in a voice-only solution
variable definitions ... 391
configure Agent Desktop behavior
variable definitions ... 371
configure Agent Desktop user settings
variable definitions ... 395
configure Agent Desktop user settings in a voice-only solution
variable definitions ... 409
configure contact timers
variable definitions ... 349
configure email server names
variable definitions ... 244
configure Event Browser
prerequisites ... 113
configure fax reply mailbox
variable definitions ... 315
configure HDX and TAPI server settings
procedure job aid ... 66
configure intrinsics
agent-supervisor barge-in ... 361
agent-supervisor observe ... 361

configure Mission Critical High Availability on the active server
variable definitions ... 502
configure Mission Critical High Availability on the standby server
variable definitions ... 504
configure notification of automatic switchovers
variable definitions ... 496
configure operating system for remote access
workgroup ... 485
configure route point
Outbound skillset ... 240
configure route point for a fax skillset
variable definitions ... 310
configure route point for an Outbound skillset
variable definitions ... 241
configure route point for a scanned document skillset
variable definitions ... 300
configure route point for a voice mail skillset
variable definitions ... 291
configure scanned document reply mailbox
variable definitions ... 305
configure service monitoring
variable definitions ... 499
configure SMS reply mailbox
variable definitions ... 338
configure SMTP server on CCMA server
variable definitions ... 142
configure Web communications
assign a development Web server name ... 343
change sequence of messages
Web communications comfort group ... 359
configure agent timers ... 348
configure customer notification log ... 350
configure intrinsics
agent-supervisor barge-in ... 361
agent-supervisor observe ... 361
configure text chat labels ... 344
configure welcome messages ... 344
create automatic phrases (Web communications) ... 351
create page push URL (Web communications) ... 353
create Web communications comfort groups ... 358
create Web On Hold comfort groups ... 356
create Web On Hold URLs groups ... 354
delete automatic phrases (Web communications) ... 352
delete message
Web communications comfort group ... 360
Web On Hold comfort group ... 357
delete page push URL (Web communications) ... 354
delete URL
Web On Hold URL group ... 355
delete Web communications comfort group ... 360
delete Web On Hold URLs group ... 356
prerequisites ... 343
configure welcome messages and text chat labels
variable definitions ... 345
configuring
configuring *(continued)*
attachment filetype restriction ... 386
Enterprise Web Chat ... 346
EWC ... 346
Landing Pads ... 177
operating system language ... 167
Web communications limits ... 350
console
administration ... 191
construct and test SQL statements or stored procedure
procedure job aid ... 72
contact center
CCMM in a voice-only solution ... 222
office hours ... 221
Contact Center applications
start ... 519
stop ... 519
Contact Center License Manager ...
Contact Center server
High Availability ... 491
Contact Center server High Availability
configure hot-standby automatic switchovers ... 499
configure hot-standby managed IP address ... 492
configure hot-standby server ... 493
configure Mission Critical High Availability ... 501
configure Mission Critical High Availability on the standby server ... 503
configure notification of automatic switchovers ... 495
configure service monitoring ... 497
monitor switchover information ... 500
prerequisites ... 492
review shadowing ... 501
start a Mission Critical Active Server ... 505
start shadowing on a Mission Critical Standby Server ... 506
stop High Availability on a Mission Critical active server ... 507
stop High Availability on a Mission Critical standby server ... 506
Contact Center Services ... 34
contact types
email ... 205
outbound ... 218
control
access to email message text ... 364
copy
voice file ... 124
copying
Event to Trap Translator settings ... 489
create
access class ... 93
alias for a recipient mailbox ... 250
automatic phrases (IM) ... 327
automatic phrases (Web communications) ... 351
closed reason ... 373
custom fields in Agent Desktop ... 367
expert group ... 330

create *(continued)*
keyword group 256
page push URL 328
page push URL (Web communications) 353
prepared responses 258
recipient mailbox 247
rule groups 270
rules 265
sender group 263
shared folder to export historical reports 142
voice file 123
voice segment 126
Web communications comfort groups 358
Web On Hold comfort groups 356
Web On Hold URLs groups 354
create and test
SQL statements 70
stored procedures 70
create expert group
variable definitions 331
create or change a keyword group
variable definitions 257
create or change an alias for a recipient mailbox
variable definitions 251
create or change prepared responses
variable definitions 260
create or change recipient mailbox
variable definitions 249
create or change rule groups
variable definitions 271
create or change rules
variable definitions 267
create or change sender group
variable definitions 264
creating offline security store 457
CS 1000
Data Extraction Tool operation 155
CS 1000 data
import 196
CS 1000 Data Extraction Tool operation
capture CDN data 161
capture IVR ACD-DN data 162
capture route data 163
capture TN data 159
capture voice port data 161
extract data
file 158
modem 157
serial connection 156
prerequisites 155
CS 100 PABX
configure 111
CS 100 PABX configuration
prerequisites 111
customer
cleanup rule 428
customer history on voice contacts
customer history on voice contacts *(continued)*
enable 385
customer notification log
configure 350
customer privacy 433
delete request 434
information request 433
custom field in Agent Desktop
delete 367
custom fields in Agent Desktop
change 367
create 367

D

data
clearing 429
management 420
purging 420
database
decrypting 472
encrypting 472
database connections
configure 66
database encryption 471
administration 470
Database Integration Wizard
configure 62
Database Integration Wizard configuration
configure database connections 66
configure data source name 63
configure HDX Provider ID 64
configure TAPI server settings 65
configure Web services 67
creating statements to access a database using SQL or stored procedures 70
prerequisites 62
remove Web service 76
update SQL statements 73
data source name
configure 63
date and time features
manage 483
default
login values 585
default closed reasons
configure 374
delete
access class 96
automatic phrases (Web communications) 352
barred email address 278
closed reason 375
custom field in Agent Desktop 367
desktop user accounts 107
document imaging server 301
email server 246
event preference 118

delete *(continued)*
fax mailbox ... 314
fax reply mailbox ... 316
fax server ... 311
geographic alternate CCT server ... 236
keyword from a keyword group ... 257
keyword group ... 258
network skillset ... 182
page push URL (Web communications) ... 354
prepared responses ... 261
recipient mailbox ... 252
rules ... 269
scanned document mailbox ... 304
scanned document reply mailbox ... 306
sender group ... 264
SMS Gateway ... 334
SMS mailbox ... 337
SMS reply mailbox ... 339
SQL statement ... 75
stored procedure ... 75
voice file ... 125
voice mail mailbox ... 295
voice mail server ... 292
voice segment ... 132
Web communications comfort group ... 360
Web On Hold URL group ... 356
delete message
Web communications comfort group ... 360
Web On Hold comfort group ... 357
delete sender
sender group ... 265
delete URL
Web On Hold URL group ... 355
deleting a site
NCC ... 174
desktop password
reset ... 105
desktop user accounts
add ... 103
delete ... 107
determine
SMTP Authentication is enabled ... 282
disable
email extended capacity ... 285
email retrieval for all mailboxes ... 288
increased email backlog capacity ... 285
rules ... 269
Windows time service ... 483
disable Auto Startup
Mission Critical HA ... 507
disabling
Agent Desktop embedded softphone ... 366
embedded softphone ... 28
disabling High Availability ... 494
disconnect
Terminal Services sessions ... 60
disconnect messages
disconnect messages *(continued)*
configure ... 326
displayed date for traffic reports
configure ... 232
DNIS Landing Pads for Universal Networking
configure ... 153
DNIS network CDNs
configure ... 188
document imaging server
add ... 300
delete ... 301
update ... 301

E

edit
port settings ... 109
email
configure ... 242
configure Open Interfaces ... 285
extended capacity ... 209
Open Interfaces ... 213
rule groups ... 206
email attachment folders
update ... 533, 571
email attachment size
specify ... 370
email backlog capacity ... 209
email configuration
add email server ... 245
barring email address ... 277
change character encoding
outgoing email ... 275
configure email server names ... 243
configure email settings ... 274
configure Microsoft Exchange for sending outgoing email ... 278
configure skillsets
email ... 247
create or change a keyword group ... 256
create or change an alias for a recipient mailbox ... 250
create or change a sender group ... 263
create or change prepared responses ... 258
create or change recipient mailbox ... 247
create or change rule groups ... 270
create or change rules ... 265
delete a barred email address ... 278
delete a keyword from a keyword group ... 257
delete a keyword group ... 258
delete a recipient mailbox ... 252
delete a rule ... 269
delete a sender group ... 264
delete email server ... 246
delete prepared responses ... 261
delete sender from a sender group ... 265
determine if SMTP Authentication is enabled ... 282
disable a rule ... 269

TLS *(continued)*
enable a rule ... 268
prerequisites ... 243
promote suggested responses ... 262
remove attachments from prepared responses ... 262
select outgoing email address ... 276
TLS
Email Manager ... 279
update the system default rule ... 253
update the system delivery failure rule ... 254
email contact type
character encoding
outgoing email messages ... 207
email rule groups ... 206
inbound email settings ... 207
Internationalized domain names ... 208
outbound email settings ... 207
recipient mailbox ... 206
email contact types
CCMA ... 212
Web services ... 212
email messages
supervisor approval ... 210
email notifications (Historical reporting)
configure ... 139
variable definitions ... 140
email rules
cleanup rule ... 426
email server
add ... 245
delete ... 246
SMTP authentication ... 281
email server names
configure ... 243
email setting
configure ... 275
email settings
configure ... 274
email traffic
reports ... 208
Emergency Help
configure ... 138
enable
customer history on voice contacts ... 385
email extended capacity ... 284
increased email backlog capacity ... 284
logon warning message ... 135
rules ... 268
SNMP traps ... 438
Web Communications transfer to skillset ... 351
encrypt database ... 470
encryption key
creating ... 471
environment variable
REST ... 80, 82, 83
event
configure ... 112
Event Browser
add event preference ... 115
change event classification ... 118
change event preference ... 117
change filtering criteria for events ... 114
delete event preference ... 118
save a list of events ... 114
sort events ... 113
start
Server Utility ... 113
view online Help for an event ... 113
Event Browser and Alarm Monitor ... 112
event classification
change ... 118
event preference
add ... 115
change ... 117
delete ... 118
events
throttle ... 116
Event severity
Critical ... 444
Information ... 444
Major ... 444
Minor ... 444
Event to Trap Translator settings
copying ... 489
Event viewer
settings ... 444
EWC
modifying chat transcripts ... 31
example
capturing terminal data ... 160
option 11C for IVR ACD-DNs output ... 163
Overlay program 23 output ... 162
Overlay program 81 output ... 161
Experience Portal ... 51
expert from files to CCMM
import ... 329
expert group
create ... 330
expert manually to CCMM
add ... 328
experts to a skillset
add ... 330
export
bulk resources ... 200
exporting ... 456
extract data
file ... 158
modem ... 157
serial connection ... 156

F

fax
configure ... 309

fax configuration
add fax mailbox ... 312
add fax server ... 310
configure fax reply mailbox ... 314
configure route point
fax skillset ... 309
delete fax mailbox ... 314
delete fax reply mailbox ... 316
delete fax server ... 311
prerequisites ... 309
update fax
system default rule ... 316
system delivery failure rule ... 317
update fax mailbox ... 313
update fax server ... 311
fax mailbox
add ... 283, 312
delete ... 314
update ... 313
fax reply mailbox
configure ... 314
delete ... 316
fax server
add ... 310
delete ... 311
update ... 311
fax system default rule
update ... 316
fax system delivery failure rule
update ... 317
features
Real-Time Statistics Multicast (RSM) ... 43
features 7.0 Feature Pack 1
add friendly name for web chat agent ... 32
Agent Desktop integration with Enterprise Web Chat ... 28
attachment filetype restriction ... 30
disabling Agent Desktop embedded softphone ... 28
force password complexity ... 31
modifying chat transcripts ... 31
removal of the default Agent Desktop Dashboard password ... 32
run one-X Communicator concurrently with Agent Desktop ... 28
Whisper Coaching ... 33
features 7.0 Feature Pack 2
increased CCMM customer contact ratio ... 30
file
extract data ... 158
filtering criteria for events
change ... 114
flag column
values ... 173
fundamentals
CCMM ... 204
CCT ... 191
language support ... 164
security ... 444

G

geographic alternate CCT server
configure ... 235
delete ... 236
grace period
reset ... 85
group of voice segments
play ... 127

H

HAI service functionality
application commands ... 40
HDX ... 38
stored procedures ... 42
HDX
HAI service functionality ... 38
HDX provider ID
configure ... 64
high availability
reinstate ... 508, 510
High Availability ... 491, 494
High Availability on a Mission Critical active server
stop ... 507
High Availability on a Mission Critical standby server
stop ... 506
High Availability solution server
renaming considerations ... 522
Historical Reporting (email contacts)
outbound contacts ... 212
Historical Reporting (outbound contacts)
outbound contacts ... 220
historical statistics collection
configure ... 186
holidays
configure ... 229
hosts file ... 537, 545, 557, 564
HOSTS file
update ... 528, 540, 549, 560, 569, 577
HOSTS file for clients
update ... 536, 541, 554, 561, 574
hotdesking
configure ... 371
hot-standby automatic switchovers
configure ... 499
hot-standby High Availability
manual switchovers ... 496
hot-standby managed IP address
configure ... 492
hot standby manual switchovers
configure ... 496
hot-standby server
configure ... 493

I

iceAdmin password 147
reset 528, 550
import
bulk resources 199
CS 1000 data 196
expert from files to CCMM 329
Windows users 194
workstations from the domain 198
import Windows users
variable definitions 195
import workstations from the domain
variable definitions 199
inbound email
settings 207
increase
email backlog capacity 209
install
Orchestration Designer 144
Windows SNMP Service 486
XML Automated Assignments feature 150
instant message
configure 326
instant message configuration
add an expert manually to CCMM 328
add experts to a skillset 330
configure disconnect messages 326
configure welcome messages 326
create automatic phrases 327
create expert group 330
create page push URL 328
import an expert from files to CCMM 329
integration
Agent Desktop with Enterprise Web Chat 28
Internationalized domain names
East Asian languages 208
IP address
change 521
IVR ACD-DN data
capture 162

J

join the server
domain 527, 549, 569

K

keyword from a keyword group
delete 257
keyword group
change 256
create 256
delete 258
keyword groups
auto-rejection of email messages 273

L

Landing Pads
configuring 177
language
levels 166
language family
compatibility 166
language support
fundamentals 164
language support fundamentals
language family compatibility 166
language levels 166
LDAP server
configure 237
lengthen
voice segment 129
length to all voice segments
add 130
remove 130
license file
update 86
license manager file on CCMS
change 88
licensing
administration 85
licensing administration
change Nodal to Corporate licensing 87
change the license manager file on CCMS 88
refresh servers 89
remote Avaya WebLM 89
reset grace period 85
update license file 86
list of access classes
preview 95
print 96
list of connected users
view 97
localized language 169
log filter settings 440
login values
default 585
log off
users 98
Voice Prompt Editor 123
log on
Server Utility 92
Voice Prompt Editor 122
logon warning message
enable 135
logon warning message title and text
configure 134
LPR port for printers
configure 149

M

mailbox
configuration ... 217
recipient ... 206
manage
date and time features ... 483
resource bulk ... 194
manually clear an alarm
Alarm Monitor ... 121
MCDN network CDNs
configure ... 187
MDB ... 418
Microsoft Exchange for sending outgoing email
configure ... 278
Microsoft Windows
configure and manage settings ... 483
Microsoft Windows configuration and management
configure operating system for remote access workgroup ... 485
disable the Windows time service ... 483
manage date and time features ... 483
verify Service Packs ... 484
Mission Critical Active Server
start ... 505
Mission Critical HA
disable Auto Startup ... 507
standby auto startup mode ... 508
Mission Critical High Availability
configure ... 501
Mission Critical High Availability on the standby server
configure ... 503
modem
extract data ... 157
modify
access class ... 94
modifying chat transcripts
Enterprise Web Chat ... 31
EWC ... 31
monitor
switchover information ... 500
monitor switchover information
procedure job aid ... 501
variable definitions ... 500
multimedia accounts
force password complexity ... 31
match the minimum password complexity criteria ... 31
Multimedia Contact Server IP address
change ... 576
Multimedia Contact Server name
change ... 566
Multimedia Contact Server name change
prerequisites ... 566
Multimedia Contact Server server name change
change the server name on the operating system ... 567
configure Agent Desktop ... 574
synchronize the operating system name
synchronize the operating system name *(continued)*
synchronize the operating system name *(continued)*
Multimedia Contact Server name ... 568
multimedia data management utility ... 424
Multimedia server settings
configure ... 535, 556

N

NCC
deleting a site ... 174
NCC server
administration ... 172
update ... 540, 560
NCC server administration
add access classes ... 175
add network skillset ... 181
add site in CCMA ... 175
add site to the NCC ... 172
configure Agent Order Preference ... 183
configure DNIS network CDNs ... 188
configure historical statistics collection ... 186
configure MCDN network CDNs ... 187
configure network communication parameters ... 178
configure network skillset properties ... 182
configure routing table assignments ... 184
configure routing tables ... 184
prerequisites ... 172
synchronize site information ... 180
network communication parameters
configure ... 178
network skillset
add ... 181
delete ... 182
network skillset properties
configure ... 182
NMS
configure ... 490
Nodal to Corporate licensing
change ... 87
notification of automatic switchovers
configure ... 495

O

Observation tone ... 34
obtain more information about alarms
Alarm Monitor ... 120
office hours
apply ... 230
configure ... 228
OFFLINE database ... 420
offline security store ... 32
online Help for an event
view ... 113
open
Alarm Monitor ... 118

open *(continued)*
voice file 124
Open Interfaces
email 213
Open Networking Open Interface 45
operating system language
configuring 167
operation
Data Extraction Tool
operation 155
operations
access classes 92
option 11C for IVR ACD-DNs output
example 163
Orchestration Designer
install 144
procedure job aid 145
outbound
configure 240
outbound campaign
cleanup rule 425
outbound campaigns
Campaign Scheduler 219
Outbound Campaign Management Tool 218
Outbound Open Interface 220
outbound configuration
configure route point
Outbound skillset 240
prerequisites 240
outbound contact type
Campaign Scheduler 219
Outbound Campaign Management Tool 218
outbound contact types
CCMA 220
Web services 220
outbound email
settings 207
Outbound Open Interface
outbound campaigns 220
process email contact types 212
Outbound skillset
configure route point 240
outgoing email address
barring 277
select 276
outgoing email messages
character encoding 207
Overlay program 23 output
example 162
Overlay program 81 output
example 161

P

PABX
record information 111
page
User Settings 394
page push URL
create 328
page push URL (Web communications)
create 353
delete 354
play
a group of voice segments 127
voice segment 127
port settings
edit 109
prepared responses
change 258
create 258
delete 261
remove attachments 262
prevent
users from accessing the server 104
preview
list of access classes 95
preview list of access classes
variable definitions 95
print
list of access classes 96
procedure job aid
Alarm Monitor appears in the foreground 120
change IP multicast setting 60
configure HDX and TAPI server settings 66
configure log filter settings 441
construct and test SQL statements or stored procedure 72
monitor switchover information 501
Orchestration Designer 145
Real-Time Reporting 138
set privileges for users 99
process email contacts
Agent Desktop 212
process email contact types
Agent Desktop 218
process outbound contacts
Agent Desktop 219
promote
suggested responses 262
properties of desktop users
change 106
purging
OFFLINE database 431

R

Real-Time Reporting
configure 136
procedure job aid 138
variable definitions 138
Real-Time Reporting (email contacts)
outbound contacts 212

Real-Time Reporting (outbound contacts)
outbound contacts ... 220
real-time traffic reports by contact
view ... 231
recipient mailbox
change ... 247
create ... 247
delete ... 252
record
voice segment ... 126
record information
PABX ... 111
re-enable
email retrieval for all mailboxes ... 288
re-enable HA
stopped services ... 508
Reference Client ... 193
refresh
Alarm Monitor ... 119
reinstate
high availability ... 510
Mission Critical high availability ... 508
Multimedia high availability ... 511
related documentation ... 21
remote Avaya WebLM ... 89
Remote Geographic Node ... 512, 513, 516
remove
administrators ... 228
all silence from all voice segments ... 131
all silence from a voice segment ... 130
specified length to all voice segments ... 130
Web communications comfort groups
WC skillset ... 234
Web On Hold comfort groups
WC skillset ... 233
Web service ... 76
remove attachments
prepared responses ... 262
rename
voice file ... 125
reporting credentials
configure ... 226
Reporting Server ... 236
reports
email traffic ... 208
traffic ... 217
reset
desktop password ... 105
grace period ... 85
iceAdmin password ... 528, 550
resource bulk
management ... 194
resource bulk management
export bulk resources ... 200
import bulk resources ... 199
import CS 1000 data ... 196
import Windows users ... 194
resource bulk management *(continued)*
import workstations from the domain ... 198
resource management
prerequisites ... 194
REST API configuration ... 79
REST API integration ... 33
restore
user access to the server ... 105
voice file ... 125
voice segment marked for deletion ... 132
REST request
add environment ... 80
creating ... 80
delete environment ... 83
deleting ... 82
testing ... 80
update environment ... 82
updating ... 82
restricting
attachment filetypes ... 386
restriction
attachment filetypes ... 30
revert
voice file (existing) ... 124
review
shadowing ... 501
RGN ... 516, 517
root certificate ... 456
Avaya Aura MS ... 476
route data
capture ... 163
route point
fax skillset
configure ... 309
scanned document skillset
configure ... 300
route point for an SMS skillset
configure ... 333
route point for a voice mail skillset
configure ... 291
routing table assignments
configure ... 184
routing tables
configure ... 184
rule groups
change ... 270
create ... 270
email ... 206
rules
change ... 265
create ... 265
delete ... 269
disable ... 269
enable ... 268

S

save a list of events
Event Browser ... 114
saving
Web communications details ... 349
scanned document
configure ... 299
scanned document configuration
add document imaging server ... 300
add scanned document mailbox ... 302
configure route point
scanned document skillset ... 300
configure scanned document reply mailbox ... 304
delete document imaging server ... 301
delete scanned document mailbox ... 304
delete scanned document reply mailbox ... 306
prerequisites ... 299
update document imaging server ... 301
update scanned document
system default rule ... 306
system delivery failure rule ... 307
update scanned document mailbox ... 303
scanned document mailbox
add ... 302
delete ... 304
update ... 303
scanned document reply mailbox
configure ... 304
delete ... 306
scanned documents system default rule
update ... 306
scanned documents system delivery failure rule
update ... 307
scheduled task ... 463, 465–467
security
fundamentals ... 444
server name change ... 521
security certificates administration ... 447
security fundamentals
CCMS Utility
view CCMS events ... 445
Event Browser and Alarm Monitor ... 445
Event severity ... 444
Event viewer settings ... 444
SNMP ... 444
security settings
configure ... 143
security store
offline ... 457
subject alternative name ... 452
security store backing up ... 449
select
CCMA, CCT and CCMM events to be forwarded ... 487
CCMA, LM, CCT and CCMM events to be forwarded 487
CCMS events to be forwarded ... 487
outgoing email address ... 276
sender group
change ... 263
create ... 263
delete ... 264
delete sender ... 265
serial connection
extract data ... 156
Serial port
configure ... 108
view ... 108
server IP address change
update CCMM server IP address in CCMA ... 544
update CCT server IP in CCMA ... 543, 563
update the server IP address in CCMA ... 541, 561
verify CCT server provider IP address ... 544, 564
verify the server IP address change ... 539, 559, 577
Server IP address change ...
Server Message Block signing ... 474
server name
change ... 521
server name change ... 527, 548
configure destination for exported scheduled reports
... 529, 550
security ... 521
verify ... 526, 547, 568
Server name change ...
server names or IP addresses change
prerequisites ... 523
server resources
view ... 110
Server utility
add desktop user accounts ... 103
change properties of desktop users ... 106
delete desktop user accounts ... 107
log off users ... 98
prevent users from accessing the server ... 104
reset desktop password ... 105
restore user access to the server ... 105
set privileges for users ... 98
view list of connected users ... 97
Server Utility
Alarm Monitor behavior
appears in background ... 120
appears in foreground ... 119
open Alarm Monitor ... 118
start Event Browser ... 113
throttle all events ... 116
service monitoring
configure ... 497
Service Packs
verify ... 484
set privileges
users ... 98
set privileges for users
procedure job aid ... 99
settings
Enterprise Web Chat ... 346

settings *(continued)*
Event viewer ... 444
inbound email ... 207
outbound email ... 207
shadowing
review ... 501
shadowing on a Mission Critical Standby Server
start ... 506
shared folder to export historical reports
create ... 142
shortcut keys
configure ... 375
shorten
voice segment ... 129
silence from a voice segment
remove ... 130
site in CCMA
add ... 175
site information
synchronize ... 180
site to the NCC
add ... 172
skillset
cleanup rule ... 426
supervisor approval for email messages ... 271
skillsets for email
configure ... 247
SMS
configure ... 332
SMS configuration
add SMS Gateway ... 333
add SMS mailbox ... 335
configure a route point
SMS skillset ... 333
configure SMS reply mailbox ... 337
delete SMS Gateway ... 334
delete SMS mailbox ... 337
delete SMS reply mailbox ... 339
prerequisites ... 332
update SMS Gateway ... 334
update SMS mailbox ... 336
update SMS system default rule ... 339
update SMS system delivery failure rule ... 340
SMS Gateway
add ... 333
delete ... 334
update ... 334
SMS mailbox
add ... 335
delete ... 337
update ... 336
SMS reply mailbox
configure ... 337
delete ... 339
SMS system default rule
update ... 339
SMS system delivery failure rule
update ... 340
SMTP Authentication
email server ... 281
SMTP server ... 462
SMTP server on CCMA server
configure ... 140
SNMP
administration ... 486
SNMP administration
configure NMS ... 490
install Windows SNMP Service ... 486
select CCMA, LM, CCT and CCMM events to be forwarded ... 487
select CCMS events to be forwarded ... 487
SNMP traps ... 438
SN system default rule
configure ... 320
social networking, configuration ... 319
Social Networking channels
configure ... 321
Social Networking configuration
configure SN system default rule ... 320
configure Social Networking channels ... 321
configure Social Networking languages ... 321
configure Social Networking mailboxes ... 322
Social Networking languages
configure ... 321
Social Networking mailboxes
configure ... 322
sort events
Alarm Monitor ... 119
Event Browser ... 113
specify
email attachment size ... 370
SQL statement
SELECT...INTO ... 42
SET NOCOUNT ON ... 42
update ... 73
SQL statement or stored procedure
delete ... 75
SQL statements or stored procedures
create and test ... 70
standby auto startup mode
Mission Critical HA ... 508
start
CCMM utility ... 224
Contact Center applications ... 519
Mission Critical Active Server ... 505
multimedia utility ... 224
shadowing on a Mission Critical Standby Server ... 506
stop
Contact Center applications ... 519
High Availability on a Mission Critical active server ... 507
High Availability on a Mission Critical standby server ... 506
stopped services
re-enable HA ... 508

stored procedures
HAI service functionality 42
subject alternative name
security store 452
suggested responses
promote 262
supervisor approval
email messages 210
supervisor approval for email messages
agent 365
skillset 271
support 26
switchover 516
switchover information
monitor 500
synchronize
site information 180
synchronize the operating system name
Voice and Multimedia Contact Server name 526
Voice Contact Server name 548
system default rule
update 253
system delivery failure rule
update 254
system license
configure 225
system locale 168

T

TAPI server settings
configure 65
text chat labels
configure 344
TFE REST configurator 80, 82
Third Call Appearance line 56
Three Call Appearance lines 56
throttle
events 116
TLS
Email Manager 279
TLS version 461
TN data
capture 159
traffic
reports 217
Transcript Filtering Web Service 346
turning off web services security 468, 524, 566
turning on web services security 460

U

update
client browsers and shared folders 534, 542, 555, 562
document imaging server 301
email attachment folders 533, 571
fax
scanned document *(continued)*
fax *(continued)*
system default rule 316
system delivery failure rule 317
fax mailbox 313
fax server 311
HOSTS file 528, 540, 549, 560, 569, 577
HOSTS file for clients 536, 541, 554, 561, 574
license file 86
NCC server 540, 560
scanned document
system default rule 306
system delivery failure rule 307
scanned document mailbox 303
SMS Gateway 334
SMS mailbox 336
SMS system default rule 339
SMS system delivery failure rule 340
SQL statement 73
system default rule 253
system delivery failure rule 254
voice mail mailbox 295
voice mail server 292
voice mail system default rule 296
voice mail system delivery failure rule 297
update CCMM server information in CCMA
variable definitions 573
update client browsers and shared folders
variable definitions 535, 543, 555, 563
update the CCMM server IP address in CCMA
variable definitions 578
update the system default rule
variable definitions 254
update the system delivery failure rule
variable definitions 255
update voice mail system default rule
variable definitions 296
update voice mail system delivery failure rule
variable definitions 298
Updating a Web service 74
use
SQL statement 42
stored procedure
SELECT...INTO 42
stored procedures
Oracle 42
user access to the server
restore 105
user configuration
User Settings page 394
user configuration in a voice-only solution
User Settings page 408
users
log off 98
set privileges 98
User Settings
configure

configure *(continued)*
configure *(continued)*
user settings 394
page 394
users from accessing the server
prevent 104
utility
CCMS network configuration 44
Nbconfig 44

V

values
flags column 173
variable definitions
add event preference 116
add fax mailbox 312
add scanned document mailbox 303
add SMS mailbox 335
add voice mail mailbox 294
Agent Desktop Displays parameters on the server 146
assign a development Web server name 344
change CS 1000 switch data 51
change IP multicast setting 60
change licensed features configuration 49
change local settings configuration 47
change SIP Local Subscriber data 53
change SIP Network Settings data 54
configure Agent Desktop Advanced Settings 387
configure Agent Desktop Advanced Settings in a voice-only solution 391
configure Agent Desktop behavior 371
configure Agent Desktop user settings 395
configure Agent Desktop user settings in a voice-only solution 409
configure a route point
SMS skillset 333
configure a route point for an SMS skillset 333
configure contact timers 349
configure email server names 244
configure fax reply mailbox 315
configure Mission Critical High Availability on the active server 502
configure Mission Critical High Availability on the standby server 504
configure notification of automatic switchovers 496
configure route point
fax skillset 310
scanned document skillset 300
configure route point for an Outbound skillset 241
configure route point for a voice mail skillset 291
configure scanned document reply mailbox 305
configure service monitoring 499
configure SMS reply mailbox 338
configure SMTP server on CCMA server 142
configure welcome messages and text chat labels 345
create expert group 331
configure route point *(continued)*
create or change a keyword group 257
create or change an alias for a recipient mailbox 251
create or change prepared responses 260
create or change recipient mailbox 249
create or change rule groups 271
create or change rules 267
create or change sender group 264
email notifications (Historical reporting) 140
import Windows users 195
import workstations from the domain 199
monitor switchover information 500
preview list of access classes 95
Real-Time Reporting 138
update CCMM server information in CCMA 573
update client browsers and shared folders 535, 543, 555, 563
update the CCMM server IP address in CCMA 578
update the system default rule 254
update the system delivery failure rule 255
update voice mail system default rule 296
update voice mail system delivery failure rule 298
verify
server name change 526, 547, 568
Service Packs 484
videos 25
view
list of connected users 97
online Help for an event 113
real-time traffic reports by contact 231
Serial port 108
server resources 110
view CCMS events
CCMS Utility 445
viewing the offline security store 459
view members
access classes 94
Voice and Multimedia Contact Server
IP address change 538
server name change 525
Voice and Multimedia Contact Server IP address change 538
Voice and Multimedia Contact Server IP address change
configure IP address 539
Voice and Multimedia Contact Server name change 524
Voice and Multimedia Contact Server name change
prerequisites 524
Voice and Multimedia Contact Server server name change
configure Agent Desktop 537
Voice Contact Server IP address change 558
Voice Contact Server IP address change
change contact center subnet IP address 558
configure the Voice Contact Server IP address 559
Voice Contact Server name change 546

Voice Contact Server name change
prerequisites ... 546
Voice Contact Server server name change
change the server name
operating system ... 546
server name in CCMA ... 531, 552
voice file
copy ... 124
create ... 123
delete ... 125
open ... 124
rename ... 125
restore ... 125
voice file (existing)
revert ... 124
voice mail
configure ... 290
voice mail configuration
add voice mail mailbox ... 293
add voice mail server ... 291
configure route point for a voice mail skillset ... 291
delete voice mail mailbox ... 295
delete voice mail server ... 292
prerequisites ... 290
update voice mail mailbox ... 295
update voice mail server ... 292
update voice mail system default rule ... 296
update voice mail system delivery failure rule ... 297
voice mail mailbox
add ... 293
delete ... 295
update ... 295
voice mail server
add ... 291
delete ... 292
update ... 292
voice mail system default rule
update ... 296
voice mail system delivery failure rule
update ... 297
voice port data
capture ... 161
Voice Prompt Editor
configure ... 122
log off ... 123
log on ... 122
Voice Prompt Editor configuration
copy voice file ... 124
create voice file ... 123
create voice segment ... 126
delete voice file ... 125
delete voice segment ... 132
lengthen or shorten a voice segment ... 129
log off the Voice Prompt Editor ... 123
log on to Voice Prompt Editor ... 122
open voice file ... 124
play a group of voice segments ... 127
Voice Prompt Editor configuration *(continued)*
play voice segment ... 127
prerequisite ... 122
record voice segment ... 126
remove all silence from all voice segments ... 131
remove all silence from a voice segment ... 130
remove or add a specified length to all voice segments ... 130
rename voice file ... 125
restore voice file ... 125
restore voice segment marked for deletion ... 132
revert to an existing voice file ... 124
search voice segment ... 128
voice segment
create ... 126
delete ... 132
lengthen ... 129
play ... 127
record ... 126
search ... 128
shorten ... 129
voice segment marked for deletion
restore ... 132

W

web chat agent
adding a friendly name ... 363
Web communications
configure ... 342
configuring limits ... 350
Web Communications
transfer to skillset ... 351
Web communications comfort group
delete ... 360
delete message ... 360
Web communications comfort groups
create ... 358
Web communications details
saving ... 349
Web On Hold comfort group
delete message ... 357
Web On Hold comfort groups
create ... 356
Web On Hold URL group
delete ... 356
delete URL ... 355
Web On Hold URLs groups
create ... 354
Web reporting
configure ... 373
Web service
remove ... 76
Web services
configure ... 67
web services security turning off ... 468, 524, 566
web services security turning on ... 460

Web statistics
configure 372
welcome messages
configure 326, 344
Whisper Skillset 34
Windows events 489
Windows SNMP Service
install 486
Windows time service
disable 483
Windows users
import 194
workstations from the domain
import 198

X

XML Automated Assignments feature
install 150