Avaya Aura® Contact Center Server Administration

Release 6.2
NN44400-610
Issue 03.07
January 2013

© 2013 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 by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

Copyright

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

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support Web site: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support Web site: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support Web site: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: New in this release 19
- Features 19
  - High Availability 19
  - SIP-enabled contact center features 21
  - Licensing 22
  - Support for inline attachments in auto suggestions and auto responses 22
  - Support for Web On Hold comfort groups 22
  - Support for Web communications comfort groups 22
  - Support for Web Communications transfer to a skillset 23
  - Support for agent-supervisor observe and barge-in 23
  - Enabling the Call Center Elite environment in Avaya Aura® Agent Desktop 23
  - Configuring Screen Pops 24
  - Enabling Customer History on Voice Contacts 24
  - Support for a Geographic Alternate Communication Control Toolkit server 24
  - Configuring a Phonebook LDAP server for voice contacts 24
- Other changes 24
  - Windows Server 2008 Release 2 support 25

Chapter 2: Introduction 27
- Prerequisites 27
- Related resources 28
  - Support 28
  - Avaya Mentor videos 28

Part I: ContactCenterManagerServer 29

Chapter 3: Contact Center Manager Server fundamentals 31
- Configuration utility 31
- Database Integration service functionality 32
- Feature report 37
- Multicast Address and Port Configuration 38
- Multicast Stream Control 38
- Server configuration 38
- Web services 39

Chapter 4: Contact Center Manager Server configuration 41
- Prerequisites to Contact Center Manager Server configuration 41
- Starting the Configuration utility with regular access level 42
- Starting the Configuration utility with administration access level 42
- Changing the local settings configuration 43
- Changing the licensed features configuration 44
- Changing the Avaya Communication Server 1000 PABX data 47
- Changing the SIP Local Subscriber data 48
- Changing the SIP Network Settings data 50

Chapter 5: Contact Center Manager Server statistics configuration 55
- Prerequisites to Contact Center Manager Server statistics configuration 55
- Configuring the Multicast controller 56
- Changing the IP multicast settings 57

Disconnecting Terminal Services sessions ... 58
Chapter 6: Database Integration Wizard configuration ... 61
Prerequisites to Database integration wizard configuration ... 61
Creating and invoking a stored procedure ... 62
Configuring the system data source names ... 63
Configuring HDX and TAPI server settings ... 64
Configuring the database connections ... 67
Configuring Web services ... 68
Removing a Web service package ... 69
Constructing and testing SQL statements or stored procedures ... 70
Updating an SQL statement ... 71
Deleting an existing SQL statement or stored procedure ... 72
Configuring the Contact Center Manager Server script ... 72
Backing up the Database Integration Service ... 73
Restoring the configuration ... 74
Part II: Contact Center Manager Server Utility ... 75
Chapter 7: Access Class operations ... 77
Prerequisites to Contact Center Manager Server Utility access class operations ... 77
Logging on to Server Utility ... 77
Creating an access class ... 78
Viewing members of an access class ... 79
Modifying access class properties ... 80
Previewing the list of access classes ... 81
Printing the list of access classes ... 81
Deleting an access class ... 82
Chapter 8: Connected user and user account operations ... 83
Prerequisites to Contact Center Manager Server Utility connected user operations ... 83
Viewing a list of connected users ... 84
Printing a list of connected users ... 84
Logging off a user ... 85
Setting privileges for a user ... 85
Adding desktop user accounts ... 91
Preventing users from accessing the server ... 92
Restoring access to the server for a user ... 93
Resetting desktop passwords ... 93
Changing the properties of a desktop user ... 94
Printing a list of users ... 95
Deleting a desktop user ... 95
Chapter 9: Serial port configuration ... 97
Prerequisites to Contact Center Manager Server Utility serial port configuration ... 97
Viewing port settings ... 97
Printing port settings ... 98
Editing port settings ... 98
Chapter 10: Server settings ... 101
Prerequisites to Contact Center Manager Server Utility server settings ... 101
Viewing server resources ... 101
Printing server resources information ... 102

Chapter 11: PABX configuration 103
Prerequisites to Contact Center Manager Server Utility PABX configuration 103
Recording PABX information 103
Chapter 12: Alarm and Event configuration 105
Prerequisites to Event Browser configuration 105
Starting the Event Browser 106
Starting the Event Browser from Server Utility 107
Sorting events in the Event Browser 108
Viewing online Help for an event 108
Saving a list of events 109
Printing a list of events 109
Changing the filtering criteria for events 110
Adding an event preference 111
Throttling all events 112
Changing an event preference 113
Printing the list of event preferences 113
Deleting an event preference 114
Changing the classification of an event 114
Opening the Alarm Monitor 115
Refreshing the Alarm Monitor 115
Sorting events in the Alarm Monitor 116
Specifying when the Alarm Monitor appears in the foreground 116
Configuring the Alarm Monitor to appear in the background 117
Obtaining more information about an alarm 117
Manually clearing an alarm 118
Chapter 13: Provider configuration 119
Starting the Provider 119
Connecting to the Contact Center Manager Server 120
Chapter 14: PC Event Browser configuration 121
Prerequisites to PC Event Browser configuration 121
Starting the PC Event Browser 121
Chapter 15: Contact Center Service Monitor configuration 123
Prerequisites to Contact Center Service Monitor configuration 124
Starting Contact Center Service Monitor 124
Changing the site to monitor 125
Exiting Networking Service Monitor 125
Refreshing the service status 126
Configuring the default site information 126
Chapter 16: Voice Prompt Editor configuration 127
Prerequisites to Voice Prompt Editor procedures 127
Logging on to the Voice Prompt Editor 128
Logging off the Voice Prompt Editor 129
Creating a voice file 129
Opening a voice file 130
Reverting to a previously saved voice file 130
Copying a voice file 131
Renaming a voice file 131

Deleting a voice file ... 131
Restoring a voice file ... 132
Creating a voice segment ... 132
Recording a voice segment ... 133
Playing a voice segment ... 134
Playing a group of voice segments ... 135
Searching for a voice segment ... 136
Lengthening or shortening a voice segment ... 137
Removing all silence from a voice segment ... 138
Removing or adding a specified length to all voice segments ... 138
Removing all silence from all voice segments ... 139
Deleting a voice segment ... 140
Restoring a voice segment marked for deletion ... 141
Part III: ContactCenterManagerAdministration ... 143
Chapter 17: Contact Center Manager Administration configuration ... 145
Prerequisites to Contact Center Manager Administration configuration ... 145
Configuring the Contact Center License Manager Service ... 146
Configuring your logon warning message title and text ... 147
Enabling the logon warning message ... 148
Configuring Real-Time Reporting ... 149
Configuring Emergency Help ... 152
Configuring e-mail notifications for Historical reporting ... 153
Configuring SMTP Server on the Contact Center Manager Administration Server ... 154
Creating a shared folder to export historical reports ... 156
Installing the Orchestration Designer ... 157
Configuring Agent Desktop Displays parameters on the server ... 158
Changing the password for the iceAdmin user account ... 160
Configuring the LPR port for printers ... 162
Configuring a network printer on the CCMA server ... 162
Configuring a network printer to use the CCMA server as the print server ... 164
Configuring a network printer to use a print server other than the CCMA server ... 166
Installing the XML Automated Assignments feature ... 167
Configuring Avaya Call Recording and Quality Monitoring ... 168
Configuring CDN Landing Pads for Universal Networking or Integrated Reporting ... 169
Configuring a DNIS Landing Pad for Universal Networking ... 170
Enabling the Avaya Aura® Call Center Elite environment in Avaya Aura® Agent Desktop ... 171
Chapter 18: Avaya Communication Server 1000 Data Extraction Tool operation. 173
Prerequisites to Avaya Communication Server 1000 Data Extraction Tool ... 173
Extracting data from a serial connection ... 174
Extracting data using a modem ... 175
Extracting data from a file ... 177
Capturing Terminal Number data ... 178
Capturing voice port data ... 179
Capturing CDN data ... 180
Capturing IVR ACD-DN data ... 181
Capturing route data ... 182
Chapter 19: Active Directory Lightweight Directory Services replication ... 183

Setting up AD-LDS replication ... 184
Choosing AD-LDS service accounts ... 186
Stopping replication on replicating servers ... 187
Starting replication on replicating servers ... 187
Chapter 20: Contact Center Manager Administration failure recovery ... 189
Prerequisites for Contact Center Manager Administration server failure recovery ... 189
Contact Center Manager Administration server failure recovery procedures ... 189
Job aid: Functionality after CCMA server failure recovery ... 191
Chapter 21: Language support fundamentals ... 193
Language levels ... 194
Language family compatibility ... 194
Chapter 22: Security Framework configuration ... 197
Prerequisites to Security Framework configuration ... 197
Configuring the Contact Center Manager Administration security details ... 198
Disabling the Security Framework ... 199
Saving the root certificate authority to a file ... 200
Importing the root certificate authority to Internet Explorer ... 200
Configuring security prompts in Internet Explorer ... 201
Viewing the security server settings ... 202
Part IV: Security Framework ... 203
Chapter 23: User identity provisioning ... 205
Adding a local user identity and password ... 205
Adding an external account (optional) ... 206
Chapter 24: Role creation and management ... 209
Creating a custom role ... 209
Deleting a custom role (optional) ... 210
Chapter 25: Element and permission mapping ... 211
Mapping elements and permissions to a role ... 211
Mapping elements and permissions by copying from another role ... 212
Removing elements from a role (optional) ... 213
Chapter 26: Role mapping ... 215
Assigning roles to a user ... 215
Assigning users to a role ... 216
Chapter 27: Policy creation and management ... 217
Creating a security policy for passwords ... 217
Chapter 28: External identity repository configuration ... 221
External identity repository configuration procedures ... 221
Provisioning an LDAP external authentication server ... 223
Provisioning a RADIUS external authentication server ... 224
Provisioning a Kerberos external authentication server ... 225
Creating the authentication scheme ... 227
Chapter 29: Element Management ... 229
Adding a new Contact Center application (optional) ... 229
Editing a secured element (optional) ... 230
Deleting a secured element (optional) ... 231
Chapter 30: Security log management ... 233

Inspecting security logs ... 233
Downloading and inspecting security logs ... 233
Reloading data from the UCM backup ... 234
Chapter 31: Account and password management ... 235
Changing your password ... 235
Resetting a user password ... 236
Disabling a user account (optional) ... 237
Reenabling a user account (optional) ... 238
Deleting a user account (optional) ... 238
Chapter 32: Session management ... 241
Viewing active sessions ... 241
Ending sessions manually ... 241
Part V: Network Control Center Server ... 243
Chapter 33: Networking Service Monitor configuration ... 245
Prerequisites to Networking Service Monitor configuration ... 245
Changing the site to monitor ... 246
Closing the Networking Service Monitor ... 246
Refreshing the service status ... 247
Setting the default site information (client machine) ... 247
Adding a site ... 247
Chapter 34: Network Control Center server administration ... 249
Prerequisites ... 249
Adding a site to the NCC ... 250
Deleting a site from the NCC ... 251
Adding access classes ... 252
Adding a site in Contact Center Manager Administration ... 253
Configuring Landing Pads for Universal Networking ... 254
Configuring network communication parameters ... 255
Synchronizing site information ... 257
Adding a network skillset ... 258
Deleting a network skillset ... 259
Configuring network skillset properties ... 260
Configuring Agent Order Preference ... 261
Configuring the routing tables ... 261
Configuring routing table assignments ... 262
Configuring the historical statistics collection ... 264
Configuring MCDN network CDNs ... 265
Configuring DNIS Network CDNs ... 266
Part VI: Communication Control Toolkit Server ... 269
Chapter 35: Communication Control Toolkit server fundamentals ... 271
Automatic Call Distribution ... 271
Communication Control Toolkit Administration Console ... 272
Communication Control Toolkit Web Administration ... 272
Trace Control Utility ... 272
Programming interfaces ... 272
Communication Control Toolkit Reference Client ... 274
Chapter 36: Communication Control Toolkit server configuration ... 275

Configuring CCT licensing ... 275
Configuring CCT deployment type ... 277
Chapter 37: Resource bulk management ... 279
Prerequisites to resource management ... 279
Importing Windows users ... 280
Importing Avaya Communication Server 1000 data ... 281
Importing workstations from the domain ... 284
Importing bulk resources ... 285
Exporting bulk resources ... 286
Part VII: ContactCenterMultimedia ... 289
Chapter 38: Contact Center Multimedia fundamentals ... 291
E-mail contact type ... 292
SMS text messages, faxes, scanned documents, and voice mail attachments ... 297
Outbound contact type ... 299
Web communications ... 302
Instant Messaging ... 302
Office hours ... 303
Chapter 39: General configuration ... 305
Prerequisites for general configuration ... 305
Configuring the system license ... 306
Configuring the reporting credentials ... 306
Adding administrators ... 307
Removing administrators ... 308
Configuring office hours ... 308
Configuring holidays ... 309
Applying office hours ... 310
Viewing real-time traffic reports by contact ... 311
Configuring the displayed date for traffic reports ... 311
Configuring Web On Hold comfort groups for a Web communications skillset ... 312
Removing a Web On Hold comfort group for a Web communications skillset ... 313
Configuring Web communications comfort groups for a Web communications skillset ... 314
Removing a Web communications comfort group from a Web communications skillset ... 314
Configuring a Geographic Alternate Communication Control Toolkit server ... 315
Deleting a Geographic Alternate Communication Control Toolkit server ... 316
Configuring an LDAP server ... 316
Configuring a Phonebook LDAP server ... 318
Configuring a Predictive server ... 319
Chapter 40: Outbound configuration ... 321
Prerequisites for Outbound configuration ... 321
Configuring a route point for an Outbound skillset ... 321
Chapter 41: E-mail configuration ... 323
Prerequisites for e-mail configuration ... 324
Configuring the e-mail server names ... 325
Adding an e-mail server ... 326
Deleting an e-mail server ... 327
Configuring skillsets for e-mail ... 328
Creating or changing a recipient mailbox ... 329

Creating or changing an alias for a recipient mailbox ... 331
Deleting a recipient mailbox ... 333
Updating the system default rule ... 334
Updating the system delivery failure rule ... 336
Creating or changing a keyword group ... 337
Deleting a keyword from a keyword group ... 339
Deleting a keyword group ... 340
Creating or changing prepared responses ... 340
Deleting prepared responses ... 343
Removing attachments from prepared responses ... 344
Promoting suggested responses ... 344
Creating or changing a sender group ... 345
Deleting a sender group ... 346
Deleting a sender from a sender group ... 347
Creating or changing rules ... 347
Enabling a rule ... 350
Disabling a rule ... 351
Deleting a rule ... 351
Creating or changing rule groups ... 352
Configuring the e-mail settings ... 353
Changing the character encoding for outgoing and incoming e-mail ... 355
Selecting the outgoing e-mail address ... 356
Barring e-mail addresses ... 357
Deleting a barred e-mail address ... 357
Configuring Microsoft Exchange for sending outgoing e-mail ... 358
Enabling SSL on the Email Manager ... 359
Enabling SMTP Authentication on your e-mail server ... 361
Determining if SMTP Authentication is enabled ... 362
Chapter 42: Voice mail configuration ... 365
Prerequisites for voice mail configuration ... 365
Configuring a route point for a voice mail skillset ... 366
Adding a voice mail server ... 367
Updating a voice mail server ... 367
Deleting a voice mail server ... 368
Adding a voice mail mailbox ... 368
Updating a voice mail mailbox ... 370
Deleting a voice mail mailbox ... 371
Updating the voice mail system default rule ... 372
Updating the voice mail system delivery failure rule ... 373
Chapter 43: Scanned document configuration ... 377
Prerequisites for scanned document configuration ... 377
Configuring a route point for a scanned document skillset ... 378
Adding a document imaging server ... 379
Updating a document imaging server ... 379
Deleting a document imaging server ... 380
Adding a scanned document mailbox ... 381
Updating a scanned document mailbox ... 382

Deleting a scanned document mailbox ... 383
Configuring a scanned document reply mailbox ... 383
Deleting a scanned document reply mailbox ... 385
Updating the scanned documents system default rule ... 385
Updating the scanned documents system delivery failure rule ... 386
Chapter 44: Fax configuration ... 389
Prerequisites for fax configuration ... 389
Configuring a route point for a fax skillset ... 390
Adding a fax server ... 391
Updating a fax server ... 391
Deleting a fax server ... 392
Adding a fax mailbox ... 392
Updating a fax mailbox ... 394
Deleting a fax mailbox ... 395
Configuring a fax reply mailbox ... 395
Deleting a fax reply mailbox ... 397
Updating the fax system default rule ... 397
Updating the fax system delivery failure rule ... 398
Chapter 45: Instant message configuration ... 401
Prerequisites for instant message configuration ... 401
Configuring welcome and disconnect messages ... 402
Creating automatic phrases ... 403
Deleting an automatic phrase ... 404
Creating a page push URL ... 404
Deleting a page push URL ... 405
Adding an expert manually to Contact Center Multimedia ... 406
Importing an expert from files to Contact Center Multimedia ... 406
Searching for users in the Active Directory ... 407
Importing an Active Directory user to Contact Center Multimedia ... 408
Creating an expert group ... 409
Deleting an expert group ... 410
Adding experts to a skillset ... 411
Deleting experts from a skillset ... 411
Chapter 46: Short Message Service configuration ... 413
Prerequisites for SMS configuration ... 413
Configuring a route point for an SMS skillset ... 414
Adding an SMS Gateway ... 415
Updating an SMS Gateway ... 415
Deleting an SMS Gateway ... 416
Adding an SMS mailbox ... 416
Updating an SMS mailbox ... 418
Deleting an SMS mailbox ... 419
Configuring an SMS reply mailbox ... 419
Deleting an SMS reply mailbox ... 421
Updating the SMS system default rule ... 421
Updating the SMS system delivery failure rule ... 422
Chapter 47: Web communications configuration ... 425

Prerequisites for Web communications configuration ... 426
Assigning a development Web server name ... 427
Configuring welcome messages and text chat labels ... 428
Configuring Web communications agent timers ... 429
Configuring customer notification log ... 431
Allowing anonymous Web communcations ... 432
Enabling Web Communications transfer to a skillset ... 432
Creating automatic phrases ... 433
Deleting an automatic phrase ... 434
Creating a page push URL ... 434
Deleting a page push URL ... 435
Creating Web On Hold URLs groups ... 436
Changing the sequence of URLs in a Web On Hold URLs group ... 437
Deleting a URL from a Web On Hold URL group ... 437
Deleting a Web On Hold URLs group ... 438
Creating Web On Hold comfort groups ... 439
Changing the sequence of messages in a Web On Hold comfort group ... 440
Deleting a message from a Web On Hold comfort group ... 440
Deleting a Web On Hold comfort group ... 441
Creating Web communications comfort groups ... 442
Changing the sequence of messages in a Web communications comfort group ... 443
Deleting a message from a Web communications comfort group ... 444
Deleting a Web communications comfort group ... 444
Configuring intrinsics for agent-supervisor observe and barge-in ... 445
Chapter 48: Predictive Outbound administration ... 447
Prerequisites ... 447
Configuring predictive blending settings ... 448
Configuring RTD Multicast settings ... 450
Configuring predictive outbound agent scripts ... 451
Chapter 49: Agent Desktop configuration ... 453
Prerequisites for Agent Desktop configuration ... 453
Resetting an agent password ... 454
Controlling access to e-mail message text ... 455
Configuring agent access to contacts ... 455
Creating or changing custom fields in Agent Desktop ... 456
Deleting a custom field in Agent Desktop ... 456
Configuring the active contact timer ... 457
Configuring the callback timer ... 458
Configuring the callback trunk access ... 458
Specifying the attachment size ... 459
Configuring Agent Desktop behavior ... 460
Configuring the state of the Agent terminal on log off ... 461
Configuring hotdesking ... 461
Configuring hotdesking in a Citrix environment ... 462
Creating or changing a closed reason ... 462
Configuring default closed reasons ... 463
Deleting a closed reason ... 464

Configuring Screen Pops ... 465
Enabling Customer History on Voice Contacts ... 466
Configuring Advanced Settings ... 467
Chapter 50: User configuration ... 471
User Settings page ... 471
Chapter 51: Data collection and management ... 475
Prerequisites for data collection and management ... 475
Starting the archive utility ... 476
Archiving by outbound campaign ... 476
Archiving by e-mail rule ... 477
Archiving by skillset ... 478
Archiving by closed reason ... 479
Restoring an archive ... 480
Recovering from a failed archive or restore ... 481
Part VIII: AvayaMediaServer ... 483
Chapter 52: Avaya Media Server configuration ... 485
Prerequisites to Avaya Media Server configuration ... 485
Logging on to Avaya Media Server Element Manager ... 485
Adding the locale-specific media content group ... 486
Uploading a batch zip file ... 487
Adding a media content group ... 488
Uploading a music media file ... 490
Uploading a treatment media file ... 491
Part IX: Managing Security ... 493
Chapter 53: Security Fundamentals ... 495
Simple Network Management Protocol ... 495
Event viewer settings ... 495
Event Browser and Alarm Monitor ... 496
Logon warning message (CCMA and UCM) ... 497
Systems Management Server security file (Multimedia) ... 497
Contact Center Manager Server Utility to view events on CCMS ... 498
Chapter 54: Platform Security ... 499
Securing the Server ... 499
Chapter 55: Security Template ... 503
Activating the Contact Center security template ... 503
Applying the security template locally on the server ... 504
Applying the security template in a network domain ... 506
Part X: Common server administration ... 507
Chapter 56: Microsoft Windows configuration and management ... 509
Managing date and time features ... 509
Disabling the Windows time service ... 510
Verifying Service Packs ... 511
Configuring the operating system for remote access in a domain ... 511
Configuring the operating system for remote access in a workgroup ... 512
Chapter 57: Simple Network Management Protocol administration ... 515
Installing Windows SNMP Service ... 515

Selecting CCMS events to be forwarded ... 516
Selecting CCMA, CCT, and CCMM events to be forwarded ... 517
Configuring the NMS ... 518
Chapter 58: Licensing administration ... 519
Resetting the grace period ... 520
Updating the license file ... 521
Changing from Nodal to Corporate licensing ... 521
Changing the licensing information on Contact Center Manager Server ... 523
Refreshing your server ... 524
Chapter 59: Contact Center database maintenance ... 525
Prerequisites to Contact Center server database maintenance ... 525
Creating a backup location ... 526
Performing an immediate backup of the database ... 527
Scheduling a backup of the database ... 529
Recovering a scheduled backup ... 531
Restoring a backup ... 531
Migrating the database ... 533
Configuring Integrated Reporting ... 534
Chapter 60: Contact Center server High Availability ... 537
Prerequisites to Contact Center Server redundancy ... 538
Configuring warm standby or hot-standby managed IP address ... 539
Configuring the warm standby or hot-standby server ... 541
Configuring the notification of automatic switchovers ... 542
Configuring warm standby or hot-standby manual switchovers ... 544
Configuring service monitoring ... 544
Configuring warm standby and hot-standby automatic switchovers ... 547
Monitoring switchover information ... 547
Reviewing shadowing ... 548
Configuring Mission Critical High Availability on the Active Server ... 549
Configuring Mission Critical High Availability on the Standby Server ... 551
Starting a Mission Critical Active Server ... 553
Starting shadowing on a Mission Critical Standby Server ... 553
Stopping High Availability on a Mission Critical Standby Server ... 554
Stopping High Availability on a Mission Critical Active Server ... 554
Disabling Auto Startup on a Mission Critical server after reboot ... 555
Selecting a startup mode on the Mission Critical Standby server after reboot ... 555
Reinstating High Availability ... 556
Chapter 61: Common procedures ... 559
Starting or stopping Contact Center applications ... 559
Stopping individual services ... 560
Starting individual services ... 560
Disabling services ... 561
Enabling services ... 561
Appendix A: Server name or IP address change ... 563
High Availability solution server renaming considerations ... 563
Prerequisites for changing server names or IP addresses ... 564
Avaya Media Server server IP address or server name change ... 564

CCMS server name change ... 565
Prerequisites for CCMS server name change ... 566
CCMS server name change procedures ... 566
Changing the server name on the operating system ... 568
Synchronizing the operating system name with the CCMS name ... 569
Verifying the server name change ... 569
Updating the HOSTS file ... 570
Joining the server to the domain ... 571
Changing the server name in the Administration tool ... 571
Configuring the Contact Management Framework settings ... 572
Configuring the Multimedia server settings ... 572
Rerunning the System Configuration ... 574
CCMS server IP address change ... 574
CCMS server IP address change procedures ... 574
Changing the contact center subnet IP address ... 576
Configuring the Contact Center Manager Server ... 577
Verifying the IP address change ... 577
Updating the Network Control Center server ... 578
Updating the HOSTS file ... 579
Updating the server IP address in CCMA ... 579
Changing the Contact Center License Manager IP address ... 580
Updating the Communication Control Toolkit license ... 581
Changing the ELAN subnet IP address ... 582
Co-resident server name change ... 582
Prerequisites for Co-resident server name change ... 583
Co-resident server name change procedures ... 583
Changing the server name in the operating system ... 586
Synchronizing the operating system name with the CCMS name ... 587
Verifying the server name change ... 587
Updating the HOSTS file ... 588
Joining the server to the domain ... 589
Resetting the iceAdmin password ... 589
Configuring destination for exported scheduled reports ... 590
Changing the server name in the Administration tool ... 591
Changing the CCT server name in the Administration tool ... 591
Changing the CCMM server name in the Dashboard ... 592
Verifying the server name change ... 593
Changing the CCMM server name in the Administration tool ... 593
Updating the HOSTS file for clients ... 594
Updating client browsers and shared folders ... 594
Configuring the Contact Management Framework ... 596
Configuring the Multimedia server settings ... 596
Co-resident server IP address change ... 598
Co-resident server IP address change procedures ... 598
Changing the contact center subnet IP address of the co-resident server ... 600
Configuring the co-resident server IP address ... 601
Verifying the server IP address change ... 601

Updating the Network Control Center server ... 602
Updating the HOSTS file ... 603
Updating the server IP address in CCMA ... 603
Updating the HOSTS file for clients ... 604
Updating client browsers and shared folders ... 605
Updating the Communication Control Toolkit server IP address in CCMA ... 606
Updating the Communication Control Toolkit provider IP address ... 606
Updating the Contact Center Multimedia server IP address in CCMA ... 607
CCMA server name change ... 607
Prerequisites for CCMA server name change ... 608
CCMA server name change procedures ... 608
Changing the server name in the operating system ... 610
Synchronizing the operating system name with the CCMA name ... 611
Verifying the server name change ... 611
Resetting the iceAdmin password ... 612
Updating historical report output files ... 613
Updating the HOSTS file for clients ... 613
Updating client browsers and shared folders ... 614
Updating the HOSTS file ... 615
Joining the server to the domain ... 616
Changing the CCMA server name in the Multimedia Dashboard ... 616
CCMA server IP address change ... 617
CCMA server IP address change procedures ... 617
Changing the server IP address on the server ... 618
Verifying the server IP address change ... 619
Updating the HOSTS file for clients ... 620
Updating client browsers and shared folders ... 621
Updating the HOSTS file ... 622
CCT server name change ... 623
Prerequisites for CCT server name change ... 623
CCT server name change procedures ... 623
Changing the server name on the operating system ... 625
Synchronizing the operating system name with the CCT name ... 626
Verifying the server name change ... 627
Updating the HOSTS file ... 627
Joining the server to the domain ... 628
Updating the CCT server name in CCMA ... 628
Configuring Contact Center Manager Server ... 629
Configuring the Multimedia server settings ... 629
Configuring the Agent Desktop ... 630
CCT server IP address change ... 631
CCT server IP address change procedures ... 631
Changing the server IP address on the operating system ... 633
Verifying the server IP address change ... 633
Updating the HOSTS file ... 634
Updating the CCT server IP address in CCMA ... 635
CCMM server name change ... 635

Prerequisites for CCMM server name change 636
CCMM server name change procedures 636
Changing the server name on the operating system 638
Changing the CCMM server name in the Dashboard 639
Synchronizing the operating system name with the CCMM name 639
Verifying the server name change 640
Updating the HOSTS file 641
Joining the server to the domain 641
Updating the e-mail attachment folders 642
Configuring the external Web server 642
Configuring the external Web server while using Webcom 6.2 (xampp 1.7.3 or higher) 644
Configuring the Agent Desktop 644
Updating the CCMM server information in Contact Center Manager Administration 645
CCMM server IP address change 646
CCMM server IP address change procedures 646
Changing the IP address on the operating system 648
Verifying the server IP address change 648
Updating the HOSTS file 649
Updating the CCMM server IP address in Contact Center Manager Administration 650
Appendix B: Default login values 651
Index 653

Chapter 1: New in this release

The following sections detail what is new in the *Avaya Aura® Contact Center Server Administration* (NN44400-610) Release 6.2.

- Features on page 19
- Other changes on page 24

Features

See the following sections for information about feature changes:

- High Availability on page 19
- SIP-enabled contact center features on page 21
- Licensing on page 22
- Support for inline attachments in auto suggestions and auto responses on page 22
- Support for Web On Hold comfort groups on page 22
- Support for Web communications comfort groups on page 22
- Support for Web Communications transfer to a skillset on page 23
- Support for agent-supervisor observe and barge-in on page 23
- Enabling the Call Center Elite environment in Avaya Aura® Agent Desktop on page 23
- Configuring Screen Pops on page 24
- Enabling Customer History on Voice Contacts on page 24
- Support for a Geographic Alternate Communication Control Toolkit server on page 24
- Configuring a Phonebook LDAP server for voice contacts on page 24

High Availability

Avaya Aura® Contact Center supports campus High Availability for fault tolerant and mission critical contact centers. Avaya Aura® Contact Center can be configured to have no single point of failure. Avaya Aura® Contact Center supports the following levels of campus high availability:

- Mission Critical High Availability
- Hot-standby High Availability
- Warm standby High Availability

Mission Critical High Availability

Avaya Aura® Contact Center supports Mission Critical High Availability for a pair of co-resident Contact Center Manager Server (CCMS) and Communication Control Toolkit (CCT) servers in a campus environment with the following:

- SIP-enabled contact center with an Avaya Aura® Communication Manager and an Avaya Aura® Session Manager.

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.

Hot-standby High Availability

Avaya Aura® Contact Center supports hot-standby High Availability for a pair of co-resident Contact Center Manager Server (CCMS) and Communication Control Toolkit (CCT) servers in a campus environment with the following:

- AML-based contact center with an Avaya Communication Server 1000 PABX. Application Module Link (AML) is an internal protocol used by Contact Center Manager Server to communicate directly with Avaya Communication Server 1000.

Warm standby High Availability

Avaya Aura® Contact Center supports warm standby High Availability for a pair of co-resident Contact Center Manager Server (CCMS) and Communication Control Toolkit (CCT) servers in a campus environment with one of the following:

- SIP-enabled contact center with an Avaya Communication Server 1000 PABX.
- SIP-enabled contact center with an Avaya Aura® Communication Manager and an Avaya Aura® SIP Enablement Services server.

Hot-standby and warm standby High Availability (HA) are configured in the same way using the High Availability utility, but they perform differently because they depend on different technologies. If a failure occurs, contact center agents with AML-based hot-standby High Availability experience a shorter downtime than agents with SIP-enabled warm standby resiliency.

High Availability solution

The level of Avaya Aura® Contact Center application High Availability you can achieve depends on your complete enterprise contact center solution. Avaya Aura® Contact Center also supports geographic disaster recovery and data resiliency.

High Availability (HA) supports resiliency for Contact Center Manager Server, Communication Control Toolkit, Contact Center Multimedia (CCMM), and Contact Center Manager Administration (CCMA).

One set of Contact Center applications (a CCMS, a CCT, a CCMA, and an optional CCMM) actively processes scripts and contacts. This set is called the active set. Another set of Contact Center applications, in the same contact center system, is running in hot standby mode. This standby set of Contact Center applications monitors and shadows active applications in the system and does not process calls. The standby CCMS monitors the active CCMS. The standby CCT monitors the active CCT. The standby CCMM monitors the active CCMM. Each active and standby pair of applications forms a resilient or replication pair. If any of the active applications fail the standby applications, running in hot standby mode, recognize this failure and start processing. The standby applications must be configured exactly the same as the active applications. Configuration changes made to the active system during normal operation are automatically copied to the standby applications. The standby applications are therefore configured correctly if they need to take over processing from the active systems. Statistical data is also automatically copied to the standby applications.

The standby CCMA is replicating the active CCMA server but CCMA services are not monitored. You must manually change over to the standby CCMA if the primary CCMA fails, since CCMA switchover is not automatic.

High Availability for CCMS, CCT and CCMM is configured using the High Availability utility in the Database Utilities. High Availability for CCMA is configured when you install CCMA.

High Availability is a licensed feature. It is enabled when a standby server license is purchased.

For more information on High Availability, see Contact Center server High Availability on page 537.

SIP-enabled contact center features

The following is a list of new features in a SIP-enabled contact center:

- Transferring DN calls to a Route Point (CDN)
- Music on hold for transfers
- Voice Screen Pop containing information about the call

In a SIP-enabled contact center, Avaya Aura® Contact Center does not support the following:

- Call Force Delay for Instant Message contacts
- Let Call Ring as an option in the Call Presentation Class of Service

Licensing

Avaya Aura® Contact Center supports WebLM. Avaya Aura® Contact Center can use WebLM to license the contact center features and to control the number of agents in your system.

You can use the License Manager Configuration utility to switch between the .lic (PLIC) and .xml (WebLM) license files. For more information, see Updating the license file on page 521.

Support for inline attachments in auto suggestions and auto responses

Administrators can add inline attachments (only as images), such as company logos, to auto suggestions and auto responses. Both standard and inline attachments are supported for auto suggestions and auto responses.

Agents can also place inline attachments (only as images) in e-mail messages.

Inline attachments display complete information within the body of the e-mail. 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.

For more information on auto suggestions and auto responses, see Creating or changing prepared responses on page 340.

Support for Web On Hold comfort groups

Web On Hold comfort groups 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.

For more information on Web On Hold comfort groups, see Creating Web On Hold comfort groups on page 439.

For more information on adding Web On Hold comfort groups to a Web communications skillset, see Configuring Web On Hold comfort groups for a Web communications skillset on page 312.

Support for Web communications comfort groups

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.

For more information on Web communications comfort groups, see Creating Web communications comfort groups on page 442.

For more information on adding Web communications comfort groups to a Web communications skillset, see Configuring Web communications comfort groups for a Web communications skillset on page 314.

Support for Web Communications transfer to a skillset

Agents can transfer a Web Communications (WC) contact to a skillset.

Important:

Agents cannot transfer a contact to a skillset that does not have active agents.

For information on enabling Web Communications transfer to a skillset, see Enabling Web Communications transfer to a skillset on page 432.

Support for agent-supervisor observe and barge-in

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 Aura® Agent Desktop (AAAD) can see all currently active Web communications and voice contacts. This display also flags any Web communications contacts where certain intrinsic values exceed the defined threshold.

For information on configuring intrinsics for agent-supervisor observe and barge-in, see Configuring intrinsics for agent-supervisor observe and barge-in on page 445.

Enabling the Call Center Elite environment in Avaya Aura® Agent Desktop

You can enable the Call Center Elite environment in Avaya Aura® Agent Desktop to manage both voice contacts from Call Center Elite and multimedia contacts from Contact Center Multimedia.

For information on enabling the Call Center Elite environment in Avaya Aura® Agent Desktop, see Enabling the Call Center Elite environment in Avaya Aura® Agent Desktop on page 171.

Configuring Screen Pops

Use the Screen Pop page to configure application shortcuts and intrinsics, while running Agent Desktop. Voice Contact Screen Pop is supported only in SIP-enabled contact centers.

For information on configuring Screen Pops, see Configuring Screen Pops on page 465.

Enabling Customer History on Voice Contacts

You can search for customer history based on the calling line ID for voice contacts.

For information on enabling Customer History on Voice Contacts, see Enabling Customer History on Voice Contacts on page 466.

Support for a Geographic Alternate Communication Control Toolkit server

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.

For information on configuring a geographic alternate CCT server, see Configuring a Geographic Alternate Communication Control Toolkit server on page 315.

Configuring a Phonebook LDAP server for voice contacts

Configuring a Phonebook LDAP server provides agents with a list of contacts during a voice call.

For information on configuring a Phonebook LDAP server, see Configuring a Phonebook LDAP server on page 318.

Other changes

See the following sections for other changes in this release:

- Windows Server 2008 Release 2 support on page 25

Windows Server 2008 Release 2 support

Contact Center server software is now supported only on Windows Server 2008 Release 2. All information about configuring Windows settings and installing the operating system are updated in this document.

For changes in procedures related to Windows Server 2008 Release 2, see the following chapters:

- Contact Center Manager Administration configuration on page 145
- Common procedures on page 559

Chapter 2: Introduction

The *Avaya Aura® Contact Center Server Administration* (NN44400-610) provides you with all information required to perform additional configuration for your Avaya Aura® Contact Center Release 6.2 servers after the initial configuration.

Prerequisites

About this task

- Read *Avaya Aura® Contact Center Overview* (NN44400-111).
- Read *Avaya Aura® Contact Center Fundamentals* (NN44400-110).
- Read *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Complete *Avaya Aura® Contact Center Installation Checklist* (NN44400-310).
- Ensure that you understand which Contact Center features you purchased.
- Install, upgrade, or migrate your Contact Center Release 6.2 software. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Commission your Contact Center Release 6.2 software. See *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Contact Center Manager Server on page 29
- Contact Center Manager Server Utility on page 75
- Contact Center Manager Administration on page 143
- Security Framework on page 203
- Network Control Center Server on page 243
- Communication Control Toolkit Server on page 269
- Contact Center Multimedia on page 289
- Managing Security on page 493
- Common server administration on page 507

Related resources

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. On the Avaya Support website at http://support.avaya.com, search for notices, release notes, downloads, user guides, and resolutions to issues. Use the Web service request system to create a service request. Chat with live agents to help answer questions. If an issue requires additional expertise, agents can quickly connect you to a support team.

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Visit http://www.youtube.com/AvayaMentor and do one of the following:

- Enter a key word or key words in the Search channel to search for a specific product or topic.
- Click the name of a playlist to scroll through the posted videos.

Part I: ContactCenterManagerServer

- Contact Center Manager Server fundamentals on page 31
- Contact Center Manager Server configuration on page 41
- Contact Center Manager Server statistics configuration on page 55
- Database Integration Wizard configuration on page 61

Chapter 3: Contact Center Manager Server fundamentals

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

Navigation

- Configuration utility on page 31
- Database Integration service functionality on page 32
- Feature report on page 37
- Multicast Address and Port Configuration on page 38
- Multicast Stream Control on page 38
- Server configuration on page 38
- Web services on page 39

Configuration utility

Use the 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 Configuration utility to add sites to the Network Control Center.

The following access levels are available:

- regular access level—Read the information in the 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.

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

- Starting the Configuration utility with administration access level on page 42.

Database Integration service functionality

The Contact Center Manager Server installation automatically installs the Database Integration service. The Database Integration service runs as a Contact Center Manager Server service when it is enabled by the license manager. When the Database Integration service starts, it

- registers as a service provider to the Host Data Exchange (HDX) service
- registers with the Telephony Application Programming Interface (TAPI) server, if TAPI is enabled in the Database Integration Wizard, and connects to the database as required to run queries and procedures

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

The Database Integration service and the Database Integration Wizard use the Common Object Request Broker Architecture (CORBA) version of the HDX interface to communicate generically with external databases, TAPI servers, or both.

Interaction of the Database Integration service with HDX

The HDX service maintains connections between registered third-party applications and Database Integration call processing.

The following is an example of the call processing script functions between the HDX service and a registered third-party application:

1. When the call processing script encounters an HDX script command (for example SEND INFO, SEND REQUEST, or GET RESPONSE), it packages the parameters into a message.
2. The HDX service receives and queues the message. A registered third-party application 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 is run, and the results are packaged into a message and is returned to the HDX.
5. When the HDX receives the message, it routes the data to call processing.
6. Call processing receives the message, unpacks the data, and maps the values to the call variable parameters of the response script function.

The Database Integration service registers with HDX as a third-party application with a unique provider ID. The provider ID is a unique ID that identifies HDX applications to Contact Center Manager Server. Contact Center Manager Server scripts use provider IDs to identify HDX applications.

After registering with HDX, the Database Integration service enables the exchange of data between the Contact Center Manager Server script and any Open Database Connectivity (ODBC) 3.51-compliant database.

You can configure the Database Integration Wizard to register the Database Integration service with the TAPI server. After you register the service with the TAPI server, you can attach data to a call.

The HDX provides a maximum of 10 client application connections. A client application refers to an application written to interact directly with the Contact Center Manager Server script. The HDX service that provides service to the third-party client applications. The Database Integration Wizard is a client of the HDX service.

Important:

Although the Database Integration Wizard is installed on the Contact Center Manager Server, the Wizard is a separate HDX client application and uses one of the 10 available HDX connections. When the Database Integration Wizard runs, nine HDX client application connections are available. The HDX limit for the size of a data parameter is 80 bytes.

When Contact Center Manager Server Database Integration is shut down, all existing registrations are released and the open connections to the Data Source Names (DSN) are closed.

Interaction with application commands

After you use the Database Integration Wizard to configure the Database Integration service, you can use call processing script commands for the HDX to integrate with the HAI service.

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

- SEND REQUEST, GET RESPONSE commands are used for database access and for data retrieval from TAPI.
- SEND INFO is used for database access and for TAPI call data attachment.

The first parameter of SEND REQUEST or SEND INFO is crucial to the operation of Database Integration Wizard. For SEND INFO, the first parameter indicates if a TAPI call data attachment needs to occur or if database access is required for the Database Integration Wizard. For SEND REQUEST, the first parameter indicates if TAPI is invoked or if the request is for database access for the Database Integration Wizard. For database access (SEND REQUEST or SEND INFO), the first parameter indicates the unique number of the SQL statement to run. For these reasons, at least one parameter is required for SEND REQUEST and SEND INFO.

SEND REQUEST

You can use the SEND REQUEST command to retrieve information from a database or from TAPI. The first parameter of the SEND REQUEST command indicates if the target is database access or TAPI. If the first parameter is %TAPI%, the system requests information from TAPI.

```
SEND REQUEST DIW_PROVIDER_ID “%TAPI%”, DATA 1
```

The system checks the parameter to determine if it corresponds to the SQL statements that you constructed using the Database Integration Wizard. If a corresponding SQL statement is found, the statement is selected to run on a Data Source Name (DSN). Stored statements are associated with particular DSNs. If a connection does not exist for the particular DSN, a connection is enabled for it. Connections are maintained for as long as the service runs.

The remaining parameters of SEND REQUEST provide information to the unknown parameters of the SQL statement (you can use up to nine parameters). The unknown parameters are identified by a question mark (?) in the SQL statement identification. Where multiple unknown parameters exist, a question mark (?) appears in the SQL statement for each unknown parameter. The HDX request must send a parameter for each question mark encountered in the SQL statement. Each question mark is replaced, in order, by the parameters in the HDX request as they are encountered. The type of each request parameter must match the data type of the SQL data field.

In the following example, the SQL statement number referenced in HAI_SQLNO_cv runs. This statement expects a single parameter (that is, it has a single question mark [?]), which is replaced by the CLID of the call when the statement runs.

```
SEND REQUEST HAI_AppID HAI_SQLNO_cv, CLID
```

GET RESPONSE

All request messages are accompanied by a GET RESPONSE message. The first parameter of the GET RESPONSE message indicates the status of the SQL statement execution. 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 script as a blank value for a string and a zero for an integer.

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 SQL statement ran successfully.
- FAILED—The SQL 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 SQL statement is of type SELECT; however, no data was returned.

The system packages the returned data in a service completion message, and passes it back to the 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 any 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 script continues without the response. Depending on the nature of the query, this can cause call handling to be disrupted.

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 parameter of the GET RESPONSE command to increase the timeout value.

In the following example, the executed SQL statement is expected to return a single piece of information, namely the ID of an agent. Use this information for direct queuing to a preferred agent. The status of the SQL execution is stored in the STRING call variable HAI_SQLRESP_cv. Configure the script to check the status of execution and use the information only if the response indicates SUCCESS.

```
GET RESPONSE HAI_AppID HAI_SQLRESP_cv, HAI_AGENTID_cv
```

SEND INFO

Use the SEND INFO command to access script and call data and attach the 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%, the SEND INFO command provides database access. In this case, the first parameter is the numeric identifier of the SQL statement to run. The numeric identifier can identify an SQL statement (such as UPDATE) that does not return data to Contact Center Manager Server. The same principles described for SEND REQUEST apply to SEND INFO when you use it for database access.

The following sample Contact Center Manager Server scripts illustrate both usages of SEND INFO.

Example 1: SEND INFO for database access

```
/* Execute SQL statement number 5 passing the current callid as parameter */
ASSIGN 5 TO HAI_SQLNO_cv
ASSIGN %CALLID% TO HAI_CALLID_cv
SEND INFO provId HAI_SQLNO_cv, HAI_CALLID_cv
```

Example 2: SEND INFO for TAPI access

```
/* Attach the text 'abandoned' to the call */
ASSIGN %TAPI% TO HAI_STRING_cv
ASSIGN ABANDONED TO HAI_DATA_cv
SEND INFO provId HAI_STRING_cv, HAI_DATA_cv
```

The previous examples illustrate scripts where the HAI service performs a single action on a voice contact processed by a script. Often, multiple HAI service actions occur sequentially in the script for a single contact. When the result of one action depends on a previous action being completed fully, ensure that the action is fully complete before the next action is executed.

You must change the following registry keys to sequentially run script 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 Database Integration service in Contact Center Manager Server supports the use of stored procedures on the database server. Stored procedures are precompiled sets of SQL statements you create in and the system stores on the database server.

The Database Integration Wizard invokes stored procedures by using conventions appropriate to the database vendor.

Creating stored procedures

You can create stored procedures on the database server by using 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

To access the feature report, click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Configuration** on the Contact Center Manager Server.

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

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.

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, and the Communication Server 1000 information.

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

- Changing the local settings configuration on page 43
- Changing the licensed features configuration on page 44
- Changing the Avaya Communication Server 1000 PABX data on page 47

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.

The following configuration utilities are available:

- Contact Center Manager Server — Configure the Contact Center server using Server Configuration.
- Configuration utility (Nbconfig)—Manage the sites and server information.
- Server Configuration utility—Manage the licensing and default settings for Avaya Aura® Contact Center.

This chapter also discusses the basic password configuration required for Contact Center Manager Server.

Prerequisites to Contact Center Manager Server configuration

- Install Contact Center Manager Server. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Commission Contact Center Manager Server. See *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Starting the Configuration utility with regular access level on page 42
- Starting the Configuration utility with administration access level on page 42
- Changing the local settings configuration on page 43
- Changing the licensed features configuration on page 44
- Changing the Avaya Communication Server 1000 PABX data on page 47

- Changing the SIP Local Subscriber data on page 48
- Changing the SIP Network Settings data on page 50

Starting the Configuration utility with regular access level

About this task

Start the 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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Network Configuration**.
2. Click each tab to view the content.
3. Click **OK**.

Starting the Configuration utility with administration access level

About this task

Start the Configuration utility with administration access level to change configuration and add sites to your networked contact center.

Procedure

1. Click **Start** > **Run**.
2. In the **Run** text box, type `nbconfig -admin`.
3. Edit the sites.
4. Click **OK**.

Changing the local settings configuration

About this task

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

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
2. In the **Server Configuration** dialog box, click the **Local Settings** tab.
3. Update the local settings.
4. Click **Apply All** or **OK**.
5. 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.
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. You must select the check box for the ELAN Subnet IP Address if you use an ELAN subnet.
Contact Center 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,

Name	Description
	and (optionally) Avaya CallPilot®) are connected.
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, networking, and predictive outbound.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
2. In the **Server Configuration** dialog box, click the **Licensing** tab.
3. Update the licensing details.
4. Click **Apply All.**
5. Click **OK**.
6. Click **Exit**.

Variable definitions

Name	Description
CCMS Package	The installation package indicates the licenses that you purchased with Contact Center: • Essential: The entry package for voice-only Contact Center on the current supported switching platforms. • Nodal Enterprise: The base package for Contact Center on the current supported switching platforms. • Corporate Enterprise: The networking package. • Corporate NCC: The Network Control Center (NCC) package for multiple Contact Center Manager Servers.
Optional Packages	You must choose the package you purchased. Packaged features includes: • 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

Name	Description
	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 Aura® Agent Desktop and configure Open Queue on the Communication Control Toolkit server. • Open Interfaces 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. • Open Interfaces 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. The system plays the greeting automatically when an agent answers a call. The Agent Greeting feature is supported only in SIP-enabled contact centers. • Offsite Agent—Use Offsite Agent to allow a Contact Center extend to an agent's preferred environment, allowing them to handle skillset calls regardless of location.
Serial Number	In an AML-based Contact Center, this is the serial number for the Avaya Communication Server 1000. You must obtain the serial

Name	Description
	number from your distributor. This value is not used in SIP-enabled contact centers.

Changing the Avaya Communication Server 1000 PABX data

About this task

Change the Avaya Communication Server 1000 PABX data after you install Contact Center Manager Server to enable communication with the Contact Center Manager Server as well as between the Avaya Communication Server 1000 PABX and Avaya CallPilot®.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
2. In the **Server Configuration** dialog box, click the **Switch CS 1000** tab.
3. Update the Avaya Communication Server 1000 PABX Data details.
4. Click **Apply All**.
5. Click **OK**.
6. Click **Exit**.

Variable definitions

Name	Description
Alternative PABX Customer Number	The customer number of the PABX, if more than one customer is registered for the PABX.
Alternative PABX IP Address	The IP address of the PABX, if more than one IP address is registered for the PABX.
Alternative PABX Serial Number	The serial number of the PABX, if more than one serial number is registered for the PABX.

Name	Description
CallPilot Alternative IP Address	The IP address of the alternate Avaya CallPilot® voice connection for the Avaya Communication Server 1000 PABX.
CallPilot Alternative Port	The port number of the alternate Avaya CallPilot® voice connection type to the Contact Center Manager Server when working with an Avaya Communication Server 1000 PABX. The default port number is 5060.
CallPilot IP Address	The IP address of the primary Avaya CallPilot® voice connection type to the Contact Center Manager Server when working with an Avaya Communication Server 1000 PABX.
CallPilot Port	The port number of the primary Avaya CallPilot® voice connection type to the Contact Center Manager Server when working with an Avaya Communication Server 1000 PABX. The default port is 5060.
PABX Customer Number	The customer number for the PABX.
PABX IP Address	The IP address of the PABX.
PABX Name	The name of the Avaya Communication Server 1000 PABX. 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.

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 may require restarting the Contact Center Manager Server. Changes to the SIP Local Subscriber data may require updates to other

Avaya Aura® Contact Center components, such as Communication Control Toolkit and Contact Center Multimedia.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **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. Click **OK**.
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 • Password	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. Password for the registration user name.
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

Name	Description
	automatically sets the specific SIP Server Type as the default. • For SIP Avaya Aura® 6.1 switch type, the default SIP Server Type is Avaya Aura® 6.1. • For SIP Avaya Communication Server 1000 switch type, the default SIP Server Type is CS1000.
MS Locale	Locale (including language and dialects) of the system environment.
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 may require restarting the Contact Center Manager Server. Changes to the SIP Local Subscriber data may require updates to other Avaya Aura® Contact Center components, such as Communication Control Toolkit and Contact Center Multimedia.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **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. Click **OK**.

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 or FQDN	If the contact center uses an Avaya Communication Server 1000 Network Routing Service (NRS), enter the IP address or Fully Qualified Domain Name (FQDN) for it here. If the contact center uses an Avaya Aura® Session Manager, enter the IP address or Fully Qualified Domain Name (FQDN) for the primary Session Manager here. If the contact center uses an Avaya Aura® SIP Enablement Services (SES) server, enter the IP address or Fully Qualified Domain Name (FQDN) for it here.
• Port	The server listening port. The default port is 5060.
• Network Transport	The SIP Network Transport communication protocol. Avaya recommends that you use TCP for Avaya Communication Server 1000.
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 or FQDN	If the contact center uses an Avaya Communication Server 1000 Signaling Server, enter the IP address or Fully Qualified Domain Name (FQDN) for it here. If the contact center uses an Avaya Aura® Application Enablement Services server, enter the IP address or Fully Qualified Domain Name (FQDN) for it here.

Name	Description
• Port	For an Avaya Communication Server 1000 the default SIP CTI Proxy Server port is 5060. 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 Communication Server 1000, the default Network Transport communication protocol is TCP. 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 or FQDN	If the contact center uses an Avaya Aura® Communication Manager and a backup Avaya Aura® Session Manager, enter the IP address or Fully Qualified Domain Name (FQDN) for 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. From the IM Provider list, select the name of the instant messaging provider. Select either Avaya Aura® Presence Services or Microsoft Office Communications Server (OCS).

Name	Description
• IP or FQDN • Port • Network Transport	The IP address or Fully Qualified Domain Name (FQDN) of the SIP IM Proxy Server. The default SIP IM Proxy Server port is 5222. The IM SIP Proxy Server transport protocol.
IM Provider	Select your IM Provider, Microsoft OCS or Avaya Aura® Presence Services.
XMPP Domain	If using an Avaya Aura® Presence Services server, enter the domain name of the Extensible Messaging and Presence Protocol (XMPP) server.

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

- Install Contact Center Manager Server. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Commission Contact Center Manager Server. See *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Configuring the Multicast controller on page 56
- Changing the IP multicast settings on page 57
- Disconnecting Terminal Services sessions on page 58

Configuring the Multicast controller

Before you begin

- Ensure that you know the Administrator password.

About this task

Configure the Multicast controller to use the IP Multicast delivery method to send Real Time Reporting data. Multicast is a network addressing method for delivering information to a group of destinations in a one-to-many distribution.

If you plan to use the Unicast delivery method, no configuration of the Contact Center Manager Server is required and you can skip this procedure.

Procedure

1. Log on to the server on which you installed Contact Center Manager Server as **Administrator**.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **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 does not support RSM compression for Contact Center Manager Server.
6. Click **Apply**.
7. Click **OK**.
8. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Multicast Address and Port Configuration**.
9. In the **RTD Multicast Configuration** dialog box, in the **Multicast IP group** box, type the multicast IP address to be used by the Contact Center Manager Server to transmit the RTD.

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

    OR

Type a new value.

11. 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

12. Click **Apply**.
13. Click **OK**.
14. Click **Start** > **All Programs** > **Administrative Tools** > **Services**.
15. Scroll down to **CCMS SDP_Service**.
16. 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. On the Contact Center Manager Server, click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Multicast Address and Port Configuration**.
2. 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.
3. In the **IP Port** boxes, type the IP port for each statistics group.
4. Change the **Multicast time to live (TTL)** value to a value that is appropriate for your network.
5. To increase or decrease the default multicast rate, in the **Multicast Rate** boxes, type a new rate in milliseconds for each port.
6. Click **OK**.

7. To activate new multicast rate settings on Contact Center Manager Server, open the Configuration utility, and click **Apply**.

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. Click **Start** > **Administrative Tools** > **Terminal Services Manager**.
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

You can use the Database Integration service to exchange call data between Contact Center Manager Server scripts and any Open Database Connectivity (ODBC)-compliant database and to attach script data to a call or multimedia contact for storage in the database.

Prerequisites to Database integration wizard configuration

- Install Contact Center Manager Server. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Commission Contact Center Manager Server. See *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Creating and invoking a stored procedure on page 62
- Configuring the system data source names on page 63
- Configuring HDX and TAPI server settings on page 64
- Configuring the database connections on page 67
- Configuring Web services on page 68
- Removing a Web service package on page 69
- Constructing and testing SQL statements or stored procedures on page 70
- Updating an SQL statement on page 71
- Deleting an existing SQL statement or stored procedure on page 72
- Configuring the Contact Center Manager Server script on page 72
- Backing up the Database Integration Service on page 73
- Restoring the configuration on page 74

Creating and invoking a stored procedure

About this task

You can create and invoke a stored procedure (a precompiled set of SQL statements stored in the database) to repeatedly to find information in the database.

Procedure

1. Create a table in the MySQL table editor.
2. Create a stored procedure using MySQL.
3. Test the stored procedure by using the MySQL test tool.
4. Configure the Database Integration Wizard with DSN access.
5. Construct your SQL statements using the Database Integration Wizard.
6. Write and activate the script.

Example of creating and invoking a stored procedure

Procedure

1. Create a table in the MySQL table editor.
2. Create a stored procedure using MySQL.

```
DROP PROCEDURE sp_GetCustomer;
delimiter |
CREATE PROCEDURE sp_GetCustomer(IN __uri VARCHAR(45),
OUT __first VARCHAR(45), OUT __last VARCHAR(45))
BEGIN
SELECT FirstName, LastName INTO __first, __last FROM
test.customers WHERE URI = __uri;
END
delimiter;
```

3. Test the stored procedure using the MySQL test tool.

```
CALL sp_GetCustomer(“customer@home.com”, @a, @b);
SELECT @a, @b;
```

4. Configure the Database Integration Wizard with DSN access.
5. Construct your SQL statements using the Database Integration Wizard.
6. Write and activate the script.

```
/*
SQLNO 3 is the number of the stored procedure as seen in the Wizard
```

```
*/
ASSIGN 3 TO HAI_SQLNO_cv
ASSIGN “customer@home.com” TO HAI_FROMADDRESS_cv
SEND INFO HAI_AppId_gv HAI_SQLNO_cv, HAI_FROMADDRESS_cv
SEND REQUEST HAI_AppId_gv HAI_SQLNO_cv
GET RESPONSE HAI_AppId_gv HAI_SQLRESP_cv,
HAI_string01_cv, HAI_string02_cv
```

Configuring the system data source names

Before you begin

- Install and configure the software and drivers to enable connection to the external database to access. You can test the database connectivity and the data access capability using the tools and techniques provided by the database vendor.

About this task

Configure the system data source names (DSN) that you want the Database Integration Wizard to use in Contact Center Manager Server before you run the Wizard. Use the ODBC Data Source Administrator to configure the system DSNs.

Procedure

1. Open Windows Explorer.
2. Navigate to the C:\Windows\SysWOW64 folder, to launch the 32-bit version of the ODBC Data Source Administrator.

   Important:

   On Win2008, the ODBC Data Source Administrator shortcut launches the 64-bit Data Source (ODBC) Administrator by default.The database integration wizard requires DSNs to be added as 32-bit.

   Important:

   Check the version of Sybase ASE ODBC Driver under the Drivers tab. The version must be 4.10.00.49. If the ODBC driver version is not 4.10.00.49, open C:\EBF11113.txt to verify if there are any error messages during the xcopy.
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, install it using the driver setup program.
6. Click **Finish**.

7. On the driver-specific setup box, in the **Data Source Name** box, type a name for the data source.
8. In the **Description** box, type a description for the data source.
9. Configure the remaining fields for connection to the database.
10. Click **OK**.
11. Click **OK** to close the ODBC Data Source Administrator window.

Configuring HDX and 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 system DSNs. See Configuring the system data source names on page 63.
- Avaya recommends that you define the provider ID as a global variable in Contact Center Manager Server. If the provider ID changes, you need not compile the script to obtain the new value.

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.

About this task

Configure HDX and TAPI server settings to configure and test the provider ID that is used to register the Database Integration service with HDX. A single provider ID is used for both database access and TAPI connectivity.

Procedure

1. On the Contact Center Manager Server, click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **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 that is used to

register the Contact Center Manager Server Database Integration service with HDX. A provider ID of 0 is invalid.

The provider ID is required in the Contact Center Manager Server script to identify the appropriate provider to which it sends information. Each HDX application must have a unique ID that identifies it to Contact Center Manager Server. No two applications at the same site can have the same provider ID. The HDX application passes the provider ID to the target server in an attempt to register with the target server software. The developer of the HDX application chooses the provider ID for the application.

4. Click **Test Connection**.
5. Review the information presented in the **Test Output and Result** box to ensure the test is successful.
6. If you do not need to integrate your software with a TAPI server, skip to step 12 on page 65.
7. In the **TAPI Connection** section, select the **Configure Tapi connection** check box.
8. In the **TAPI Server HostName** box, type the host name or the IP address of the TAPI server.
9. 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 port to be specified. Consult your TAPI configuration to determine the actual port.

   Important:

   If TAPI is co-resident with Contact Center Manager Server, ports 5000 to 5010 are not available for use. You must select another port outside of the 5000 to 5010 range.
10. Click **Test Connection**.
11. 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.
12. Click **Next**.

    Important:

    To configure the database connections now, see the procedure to configure the database connections.

13. On the Configure Database Connections window, click **Next**.
14. On the Configure Web Services window, click **Next**.
15. On the Construct SQL Statements window, click **Next**.
16. 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 may 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 the database connections

Before you begin

- Ensure that you have the correct access permissions to the database.
- If you are already on the Configure Database Connections window, skip to step 4 on page 67.

About this task

Configure the database connections to configure a user name and password pair for each DSN and to test the connections.

Procedure

1. On the Contact Center Manager Server, click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **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 configure a connection to from the tree view.
5. In the **Username** box, type the user name for the selected DSN.
6. In the **Password** box, type the password for the selected DSN.
7. Click **Test Connection**.
8. Review the information presented in the **Test Output and Result** box to ensure the test is successful.

   Important:

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

   Important:

   To configure Web services now, review the procedure to configure Web services.
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

- Ensure that you have access to the Web Service Description Language (WSDL) document that describes the Web service. By providing the Uniform Resource Locator (URL) to the WSDL document, the Database Integration Wizard can generate a corresponding set of stored procedures that use the Web service.
- If you are already on the Configure Web Services window, skip to step 5 on page 68.

About this task

Configure Web services to import Web service functionality.

Important:

A limitation exists on the range of Web services that you can import. 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, due to the limitation that an SQL query can only accept a fixed number of simple data types.

Procedure

1. On the Contact Center Manager Server, click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **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 Web Service Description Language (WSDL) document that describes the Web service.
6. In the **Package Name** box, type a unique name for the Web service package.
7. If the Web service uses SSL/TLS security (for example, https://), in the **X.509 Certificate (Secure Web Services)** box, type the location of the X.509 certificate.

   OR

   Click **Browse** to navigate to the X.509 certificate.
8. Click **Import WSDL**.
   The import process can take some time, depending on the size of the WSDL document being processed. After you import WSDL, a summary of the imported procedures appears in the Package Summary and Result box. If the import is not successful, the reason for the failure appears in the box.

9. Click **Next**.

   Important:

   To configure SQL statements now, review the procedure for Constructing and testing SQL statements or stored procedures.

10. On the Construct SQL Statements window, click **Next**.
11. On the Complete window, click **Finish**.

Removing a Web service package

About this task

Remove a Web service package that you no longer require by using the Database Integration Wizard.

Procedure

1. On the Contact Center Manager Server, click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **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. Close the Database Integration Wizard.

Constructing and testing SQL statements 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 70.

About this task

Construct and test a new SQL statement or stored procedure (or test an existing SQL statement or stored procedure) to ensure the SQL code works to locate content in the database.

Procedure

1. On the Contact Center Manager Server, click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **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 **Edit statement here** box, type the SQL statement or the stored procedure.

   The statement must contain valid sample data for variable parameters.
7. Select the DSN on which you want to configure an SQL statement from the tree view.
8. Click **Test Execute**.
9. In the **UserName** box, type the user name for the selected DSN.
10. In the **Password** box, type the password for the selected DSN.
11. Click **Test Connection**.
12. If the test is successful, replace the variable parameters of the statement with question marks (?), and then click **Add** to add the statement to the DSN for later selection by the Contact Center Manager Server Database Integration service.
13. Click **Next**.
14. 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.

Updating an SQL statement

About this task

Update an SQL statement to correct errors or change the SQL statement.

Procedure

1. On the Contact Center Manager Server, click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **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 or stored procedure.
   The selected statement or stored procedure appears in the Edit statement here box.
7. Edit the statement.
8. Click **Test Execute** to test the statement.
9. If the test is successful, replace the variable parameters of the statement with question marks (?), and then click **Update**.
10. Click **Next**.
11. On the Complete window, click **Finish** to accept the changes and close the wizard.

Deleting an existing SQL statement or stored procedure

About this task

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

Procedure

1. On the Contact Center Manager Server, click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **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 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.

Configuring the Contact Center Manager Server script

Before you begin

- Use a global variable rather than a call variable for the Application ID. In this example, the call variable is used for testing.
- Use the return value from the database operation only if the operation was successful.
- Assign values to HDX variables before you use them in an HDX command.

About this task

Configure the Contact Center Manager Server script to use the newly enabled function.

Use a Contact Center Manager Server client to edit the Contact Center Manager Server scripts. The HDX scripting commands are added using the provider ID, the numerical identifier, and the parameters you identified when you configured your database connections.

Procedure

1. Create the call variables for passing data to and for retrieving data from the database.
2. Write and activate the script.
3. Test the script using physical calls. Ensure that the full required behavior is observed. If you do not see the required behavior, examine the trace files for the Database Integration Wizard.

Backing up the Database Integration Service

Before you begin

- Ensure that you export only the ODBC DSNs created for use with the Database Integration Wizard. Some Contact Center Manager Server DSNs reference a computer host name or IP address. If you export the entire ODBC folder and restore these DSNs after an IP address or host name change, the server can malfunction.

About this task

Back up the Database Integration Service to back up the current configuration.

Avaya recommends that you manually back up the current configuration and that you refresh the backups after using the Database Integration Wizard to make changes. The Database Integration Wizard backup and restore is not included in the Contact Center Manager Server backup and restore process.

Procedure

1. On the Contact Center Manager Server, click **Start** > **Run**.
2. In the **Open** box, type `regedit`.
3. Click **OK**.
4. In the **Registry Editor**, open the key \HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Nortel\ICCM\HAI
5. From the **File** menu, select **Export**.
6. In the **Export Registry File** dialog box, type a name and location in which to store the configuration file.
7. Click **Save**.
8. In the **Registry Editor**, open the key \HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC
9. From the **File** menu, select **Export**.

10. In the **Export Registry File** dialog box, type a suitable name and location to use for storing the ODBC configuration file.
11. Click **Save**.
12. Close the **Registry Editor**.

Restoring the configuration

Before you begin

- Perform an ODBC restore only if the server name and IP address are unchanged, and the ODBC configuration remains unchanged since the ODBC backup operation occurred. If either condition is true, perform a new backup.

About this task

Restore the configuration from a previous backup.

Procedure

1. On the Contact Center Manager Server, click **Start** > **Run**.
2. In the **Open** box, type `regedit`.
3. Click **OK**.
4. On the **Registry Editor** dialog box, click **File** > **Import**.
5. On the **Import Registry File** dialog box, select a previously saved HAI configuration file.
6. In the **Import Registry File** dialog box, select a previously saved ODBC configuration file.
7. Click **Open**.
8. On the **Registry Editor** message box, click **OK**.

Part II: Contact Center Manager Server Utility

- Access Class operations on page 77
- Connected user and user account operations on page 83
- Serial port configuration on page 97
- Server settings on page 101
- PABX configuration on page 103
- Alarm and Event configuration on page 105
- Provider configuration on page 119
- PC Event Browser configuration on page 121
- Contact Center Service Monitor configuration on page 123
- Voice Prompt Editor configuration on page 127

Chapter 7: 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 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.

Prerequisites to Contact Center Manager Server Utility access class operations

- Install and commission Server Utility. See *Avaya Aura® Contact Center Installation* (NN44400-311) and *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Logging on to Server Utility on page 77
- Creating an access class on page 78
- Viewing members of an access class on page 79
- Modifying access class properties on page 80
- Previewing the list of access classes on page 81
- Printing the list of access classes on page 81
- Deleting an access class on page 82

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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Server Utility** > **Server Utility**.
2. On the 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 77.

About this task

Create an access classes from the Server Utility window. You can also add access classes using the Contact Center Manager Administration (CCMA) client. For information about adding access classes in Contact Center Manager Administration, see the Contact Center Manager Administration online Help.

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 79 and step 8 on page 79 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 77.

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, click **Cancel**.
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 77.
- Create the access classes to modify. See Creating an access class on page 78.
- Configure users in CCMA. See *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

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 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 80 and step 9 on page 80 for each function to which you want this access class to have access.
11. Click the **Members** tab.
12. Add the members to 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 77.

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 77.

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 77.

About this task

Delete an access class that you no longer use.

Important:

You cannot delete the default access classes (“AdminGroup”, 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 8: 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

- Install and commission Server Utility. See *Avaya Aura® Contact Center Installation* (NN44400-311) and *Avaya Aura® Contact Center Commissioning* (NN44400-312).
- Log on to Server Utility. See Logging on to Server Utility on page 77.

Navigation

- Viewing a list of connected users on page 84
- Printing a list of connected users on page 84
- Logging off a user on page 85
- Setting privileges for a user on page 85
- Adding desktop user accounts on page 91
- Preventing users from accessing the server on page 92
- Restoring access to the server for a user on page 93

- Resetting desktop passwords on page 93
- Changing the properties of a desktop user on page 94
- Printing a list of users on page 95
- Deleting a desktop user on page 95

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**.

Printing a list of connected users

About this task

Print a list of users connected to the Contact Center Manager Server to produce a hard copy of the list recorded in the Avaya Aura® Contact Center.

Procedure

1. From the Server Utility window, click **System Administration** > **System Configuration**.
2. Double-click **Connected Sessions**.
3. In the Connected Sessions window, choose **File** > **Print**.
4. Choose the options for your printer.
5. Click **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, click **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 91.
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 94.

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.

Function	Privilege	Description
	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.
	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, and delete event preferences.

Function	Privilege	Description
Formulas	View	View formulas for statistical reports.
	Edit	View and modify formulas for statistical reports.
	Create/Delete	Create and 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 and delete IVR ACD-DNs.
Network Communication Parameters	View	View Network Communication Parameters.
	Edit	View and modify Network Communication Parameters.
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.

Function	Privilege	Description
	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.
	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.

Function	Privilege	Description
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 NNC.
	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.
	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.

Function	Privilege	Description
	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 78.

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 *Avaya Aura® Contact Center Performance Management* (NN44400-710).

If adding a new desktop user account in a contact center that uses the High Availability feature it may take up to six hours before the new user is created on the standby CCMS server. If the active server switches over to the standby server during this interval this new desktop user account may not exist or if it exists it may not be able to access the CCMS database. Avaya recommends adding the desktop user account again after switchover.

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 94.

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.

Printing a list of users

About this task

Print a list of users to keep as an easy reference in company records.

Procedure

1. On the Server Utility window, double-click **User Administration**, and then double-click **Users**.
2. From the Users window, choose **File** > **Print**.
3. Select the printer and the printer options.
4. Click **OK**.

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**.

Chapter 9: 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, print, 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

- Install and commission Server Utility. See *Avaya Aura® Contact Center Installation* (NN44400-311) and *Avaya Aura® Contact Center Commissioning* (NN44400-312).
- Log on to Server Utility. See Logging on to Server Utility on page 77.

Navigation

- Viewing port settings on page 97
- Printing port settings on page 98
- Editing port settings on page 98

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**.

Printing port settings

About this task

Print the port settings.

Procedure

1. In the Server Utility window, expand **System Administration**.
2. Expand **System Configuration**.
3. Double-click **Serial Ports**.
4. Click **File** > **Print**.
5. Select the printer and the printer options.
6. Click **OK**.

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. From the Serial Ports window, click **File** > **Edit**.
5. On the Serial Ports window, select a configured serial port.
6. Click **File** > **Properties**.

7. Configure the changes to the properties of the Serial Port.

Chapter 10: Server settings

This chapter describes how to view and print 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

- Install and commission Server Utility. See *Avaya Aura® Contact Center Installation* (NN44400-311) and *Avaya Aura® Contact Center Commissioning* (NN44400-312).
- Log on to Server Utility. See Logging on to Server Utility on page 77.

Navigation

- Viewing server resources on page 101
- Printing server resources information on page 102

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 **Start** menu, click **All Programs** > **Avaya** > **Contact Center** > **Server Utility** > **Server Utility**.
3. On the Server Utility window, expand **System Administration.**

4. Expand **System Configuration**.
5. Double-click **Server Settings**.

Printing server resources information

About this task

Print server resource information to document in paper format the system configuration of your contact center for company records.

Procedure

1. Log on to the server where the Server Utility is installed.
2. On the **Start** menu, click **All Programs** > **Avaya** > **Contact Center** > **Server Utility** > **Server Utility**.
3. On the Server Utility window, expand **System Administration.**
4. Expand **System Configuration**.
5. Double-click **Server Settings**.
6. Click **File** > **Print**.
7. Select the printer and the printer options.
8. Click **OK**.

Chapter 11: 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

- Install and commission Server Utility. See *Avaya Aura® Contact Center Installation* (NN44400-311) and *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Recording PABX information on page 103

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 may not be applicable and therefore be 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. Enter an optional **Description**.
8. Click **Close**.

Chapter 12: 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. For more information about these features, see Procedure job aid on page 106.

To view client events, such as successful logon or logoff or failure to connect, use the PC Event Browser.

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

- Install and commission Server Utility. See *Avaya Aura® Contact Center Installation* (NN44400-311) and *Avaya Aura® Contact Center Commissioning* (NN44400-312).
- Log on to Server Utility. See Logging on to Server Utility on page 77.

Navigation

- Starting the Event Browser on page 106
- Starting the Event Browser from Server Utility on page 107
- Sorting events in the Event Browser on page 108
- Viewing online Help for an event on page 108

- Saving a list of events on page 109
- Printing a list of events on page 109
- Changing the filtering criteria for events on page 110
- Adding an event preference on page 111
- Throttling all events on page 112
- Changing an event preference on page 113
- Printing the list of event preferences on page 113
- Deleting an event preference on page 114
- Changing the classification of an event on page 114
- Opening the Alarm Monitor on page 115
- Refreshing the Alarm Monitor on page 115
- Sorting events in the Alarm Monitor on page 116
- Specifying when the Alarm Monitor appears in the foreground on page 116
- Configuring the Alarm Monitor to appear in the background on page 117
- Obtaining more information about an alarm on page 117
- Manually clearing an alarm on page 118

Starting the Event Browser

About this task

Start the Event Browser to view a history of events that occurred on the CCMS server.

Procedure

Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Server Utility** > **PC Event Browser**.

Procedure job aid

Table 1: Event Browser versus Alarm Monitor features

Feature	In Event Browser?	In Alarm Monitor?
View events	Yes	Yes

Feature	In Event Browser?	In Alarm Monitor?
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

Starting the Event Browser from Server Utility

Before you begin

- Log on to Server Utility. See Logging on to Server Utility on page 77.

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 107.

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 107.

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, double-click 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 110.
- Open the Event Browser. See Starting the Event Browser from Server Utility on page 107.

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**.

Printing a list of events

Before you begin

- Open the Event Browser. See Starting the Event Browser from Server Utility on page 107.

About this task

Print a record of events for technical support.

Procedure

1. On the Events Browser window, click **File** > **Print**.
2. Select the printer and printer options.
3. 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 107.

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, 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 107.

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 107.

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 may 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. Expand **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 107.

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 Event Browser window, select the **Event Preferences** to change.
2. Click **File** > **Event Details**.

Printing the list of event preferences

Before you begin

- Open the Event Browser. See Starting the Event Browser from Server Utility on page 107.

About this task

Print the list of event preferences for your records.

Procedure

1. From the Event Preferences window, click **File** > **Print**.
2. Configure the printer and print settings.
3. Click **OK**.

Deleting an event preference

Before you begin

- Open the Event Browser. See Starting the Event Browser from Server Utility on page 107.

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 107.

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 77.

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 115.

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 115.

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 77.

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 77.

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 115.

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 115.

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 13: Provider configuration

The Provider application receives Contact Center script information over the Host Data Exchange (HDX) interface between the Contact Center Manager Server and the Contact Center Manager Administration server.

Navigation

- Starting the Provider on page 119
- Connecting to the Contact Center Manager Server on page 120

Starting the Provider

Before you begin

- Ensure that you have administrative privileges on the server on which Server Utility is installed.

About this task

Start the Provider to receive Contact Center scripts.

Procedure

1. Log on to the server on which Server Utility is installed.
2. Select **Start** > **All Programs** > **Avaya** > **Contact Center** > **Server Utility** > **Provider**.

Connecting to the Contact Center Manager Server

Before you begin

- Ensure that you know the Contact Center Manager Server IP address.
- Ensure that you know provider ID. The provider ID must match the ID in the Contact Center script.
- Ensure the Provider is started. See Starting the Provider on page 119.

About this task

You can configure Provider to return information to the Contact Center script. The receiving side receives both SEND INFO and SEND REQUEST information from the Contact Center script. Configure the sending side to send a variety of information to the Contact Center script. The Contact Center script command GET RESPONSE receives the information sent by Provider.

Procedure

1. In the **Server Site IP Address** box, type the IP or computer name of the Contact Center Manager Server.

   If the Provider and the Contact Center Manager Server reside on the same computer, you can use the IP address 127.0.0.1.
2. Click **Connect to Server**.
   The Register button is enabled.
3. In the **Enter Register ID** box, type the provider ID of the application.
4. Click **Register** to assign the value.

Chapter 14: PC Event Browser configuration

Use the PC Event Browser to view events that occur on the client computers. You cannot view events that occur on the server in PC Event Browser.

Prerequisites to PC Event Browser configuration

- Ensure that you have administrative privileges on the server on which you installed Server Utility.

Navigation

- Starting the PC Event Browser on page 121

Starting the PC Event Browser

About this task

Start PC Event Browser.

Procedure

1. Log on to the server on which Server Utility is installed.
2. Click **Start** > **Avaya** > **Contact Center** > **Server Utility** > **PC Event Browser**.

Chapter 15: Contact Center Service Monitor configuration

You can use Service Monitor to monitor the state of services at the Network Control Center (NCC) and across multiple Contact Center Manager Servers on the NCC.

Services are divided into two categories:

- Core Services
  - Agent Skillset Manager (ASM)
  - Telephony Services Manager (TSM)
  - Meridian Link Services (MLS) Manager
  - Task Flow Executor (TFE)
  - Voice Services Manager (VSM)
- Database Services
  - Operations, Administration and Maintenance Auditing (Audit)
  - Event Broker (EB)
  - Event Server (ES event server is not on every computer so this is not checked against the monitor lights)
  - Historical Data Collector (HDC)
  - Historical Data Manager (HDM)
  - Intrinsic Server (IS)
  - Operations, Administration, and Maintenance (OAM)
  - NCC Operations, Administration, and Maintenance (NCCOAM)
  - Nodal Operations, Administration, and Maintenance (NDLOAM)
  - Real-Time Data Collector (RDC)
  - Real-Time Statistics Multicast (RSM)
  - Statistical Data Manager Configuration Administrator (SDMCA)
  - Server Data Propagator (SDP)
  - Task Flow Access (TFA)

On the NCC, the services that can be running and monitored are limited to the following:

- Audit
- HDM
- OAM
- TSM
- NCCOAM

Prerequisites to Contact Center Service Monitor configuration

- Install and commission the Network Control Center. See *Avaya Aura® Contact Center Installation* (NN44400-311) and *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Starting Contact Center Service Monitor on page 124
- Changing the site to monitor on page 125
- Exiting Networking Service Monitor on page 125
- Refreshing the service status on page 126
- Configuring the default site information on page 126

Starting Contact Center Service Monitor

About this task

Start Contact Center Service Monitor.

Procedure

1. Log on to the server on which Server Utility is installed.
2. Click **Start** > **Avaya** > **Contact Center** > **Server Utility** > **Service Monitor**.

Changing the site to monitor

Before you begin

- Start Contact Center Service Monitor. See Starting Contact Center Service Monitor on page 124.

About this task

Monitor the service status of other servers in the network.

Procedure

1. In the left pane, double-click **Other Sites**.
2. In the expanded list, double-click the site to monitor.

Exiting Networking Service Monitor

Before you begin

- Start Contact Center Service Monitor. See Starting Contact Center Service Monitor on page 124.

About this task

Exit the application to close the Service Monitor icon in the Windows system tray.

Procedure

1. In the **System** tray, right-click the **Contact Center Service Monitor** icon.
2. From the menu, select **Exit Contact Center Service Monitor**.

Refreshing the service status

Before you begin

- Launch Contact Center Service Monitor. See Starting Contact Center Service Monitor on page 124.

About this task

Refresh the status of services.

Procedure

Click **Refresh Service Status**.

Configuring the default site information

Before you begin

- Start Contact Center Service Monitor. See Starting Contact Center Service Monitor on page 124.

About this task

Configure the default monitored site.

Procedure

1. Click **Set Site**.
2. In the **Set IP Address of Server** dialog box, in the **CLAN IP** address box, type the IP address of the site to configure it as the default site.
3. Click **OK**.
4. Restart **Contact Center Server Monitor** for the changes to take effect.

Chapter 16: 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

- Ensure that you are connected to Avaya Communication Server 1000.

Navigation

- Logging on to the Voice Prompt Editor on page 128
- Logging off the Voice Prompt Editor on page 129
- Creating a voice file on page 129
- Opening a voice file on page 130
- Reverting to a previously saved voice file on page 130
- Copying a voice file on page 131
- Renaming a voice file on page 131
- Deleting a voice file on page 131
- Restoring a voice file on page 132
- Creating a voice segment on page 132
- Recording a voice segment on page 133
- Playing a voice segment on page 134
- Playing a group of voice segments on page 135

- Searching for a voice segment on page 136
- Lengthening or shortening a voice segment on page 137
- Removing all silence from a voice segment on page 138
- Removing or adding a specified length to all voice segments on page 138
- Removing all silence from all voice segments on page 139
- Deleting a voice segment on page 140
- Restoring a voice segment marked for deletion on page 141

Logging on to the Voice Prompt Editor

Before you begin

- Log on to Server Utility. See Logging on to Server Utility on page 77.

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 128.

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 128.

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 128.

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 128.
- Open a voice file and make changes to it. See Opening a voice file on page 130.

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 128.
- 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 128.
- 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 128.
- 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 128.
- 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 128.
- Open a voice file. See Opening a voice file on page 130.

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 128.
- Create a voice segment. See Creating a voice segment on page 132.

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 133 to step 6 on page 133.
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 128.
- Create a voice segment. See Creating a voice segment on page 132.
- Record a voice segment. See Recording a voice segment on page 133.

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 128.
- Create a voice segment. See Creating a voice segment on page 132.
- Record a voice segment. See Recording a voice segment on page 133.

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 135 to step 3 on page 135 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 128.
- Create a voice segment. See Creating a voice segment on page 132.
- Record a voice segment. See Recording a voice segment on page 133.

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 128.
- Create a voice segment. See Creating a voice segment on page 132.
- Record a voice segment. See Recording a voice segment on page 133.

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 128.
- Create a voice segment. See Creating a voice segment on page 132.
- Record a voice segment. See Recording a voice segment on page 133.

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 128.
- Create a voice segment. See Creating a voice segment on page 132.
- Record a voice segment. See Recording a voice segment on page 133.

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 128.
- Create a voice segment. See Creating a voice segment on page 132.
- Record a voice segment. See Recording a voice segment on page 133.

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 128.
- Create a voice segment. See Creating a voice segment on page 132.
- Record a voice segment. See Recording a voice segment on page 133.

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 128.
- Create a voice segment. See Creating a voice segment on page 132.
- Record a voice segment. See Recording a voice segment on page 133.

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 III: ContactCenterManagerAdministration

- Contact Center Manager Administration configuration on page 145
- Avaya Communication Server 1000 Data Extraction Tool operation on page 173
- Active Directory Lightweight Directory Services replication on page 183
- Contact Center Manager Administration failure recovery on page 189
- Language support fundamentals on page 193
- Security Framework configuration on page 197

Chapter 17: 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 Manager Administration – Client Administration* (NN44400-611).

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

- Install Contact Center Manager Administration server. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Commission Contact Center Manager Administration server. See *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Configuring the Contact Center License Manager Service on page 146
- Configuring your logon warning message title and text on page 147
- Enabling the logon warning message on page 148
- Configuring Real-Time Reporting on page 149
- Configuring Emergency Help on page 152
- Configuring e-mail notifications for Historical reporting on page 153

- Configuring SMTP Server on the Contact Center Manager Administration Server on page 154
- Creating a shared folder to export historical reports on page 156
- Installing the Orchestration Designer on page 157
- Configuring Agent Desktop Displays parameters on the server on page 158
- Changing the password for the iceAdmin user account on page 160
- Configuring the LPR port for printers on page 162
- Configuring a network printer on the CCMA server on page 162
- Configuring a network printer to use the CCMA server as the print server on page 164
- Configuring a network printer to use a print server other than the CCMA server on page 166
- Installing the XML Automated Assignments feature on page 167
- Configuring Avaya Call Recording and Quality Monitoring on page 168
- Configuring CDN Landing Pads for Universal Networking or Integrated Reporting on page 169
- Configuring a DNIS Landing Pad for Universal Networking on page 170
- Enabling the Avaya Aura® Call Center Elite environment in Avaya Aura® Agent Desktop on page 171

Configuring the Contact Center License Manager Service

Before you begin

- Ensure that the Contact Center Manager Administration server software is installed on a stand-alone server.
- Ensure that you have administrator privileges on the Contact Center Manager Administration server.

About this task

Configure the Contact Center License Manager Service for the Report Creation Wizard component to function if your Contact Center Manager Administration server is not co-resident with another Contact Center application.

If you installed the Contact Center Manager Administration server software co-resident with Contact Center Manager Server, the IP address and port number are set up by the Contact Center Manager Server installation procedure.

Procedure

1. Log on to the Contact Center Manager Administration server as an administrator.

2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Configuration**.
3. In the left pane, navigate to **Avaya** > **Applications** > **LM Service Configuration**.
4. In the right pane, click the **LM Service Configuration** icon.
5. In the **LM Service - Configuration Setup** dialog box, in the **Primary Server's IP Address** boxes, type the IP address for the primary Contact Center License Manager server.
6. In the **Primary Server's Port** box, type port number for the primary Contact Center License Manager server.
7. If you have a standby Contact Center License Manager server, in the **Standby Server's IP Address** boxes, type the IP address for the standby Contact Center License Manager server.
8. If you have a standby Contact Center License Manager server, in the **Standby Server's Port** box, type the port number for the standby Contact Center License Manager server.
9. Click **OK** to submit the information.
10. In the **LM Service - Configuration Setup** dialog box, click **OK**.
11. In the dialog box that prompts you to restart the Contact Center License Manager Service, click **Yes**.
12. Click **OK**.
13. Close all windows.

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 2008 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.

If you enable the Security Framework, the logon message is overridden.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Click **Start** > **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 147.

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 149.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **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.

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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **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 (10 000).
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 150.
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 may 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 may 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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **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 e-mail notifications for Historical reporting

Before you begin

- Check with the Administrator of the e-mail 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.
- Install Internet Information Services (IIS) on the Contact Center Manager Administration Server. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Install Microsoft Active Directory Application Mode on the Contact Center Manager Administration Server. See *Avaya Aura® Contact Center Commissioning* (NN44400-312).

About this task

Configure Simple Mail Transfer Protocol (SMTP) to send an e-mail 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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **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 154.
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 153.
8. For **Username**, enter the e-mail user name.
9. For **Password**, enter the e-mail user password.
10. If the SMTP Server requires SSL, select **SSL Required**.
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 e-mail address from which notifications are sent.
Authentication Required	Select if the SMTP server requires authentication.
User Name	The e-mail user name.
Password	The e-mail user password.
Enable SSL	Select if the SMTP server requires SSL.

Configuring SMTP Server on the Contact Center Manager Administration Server

Before you begin

- Install Internet Information Services (IIS) on the Contact Center Manager Administration Server. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Install Microsoft Active Directory Application Mode on the Contact Center Manager Administration Server. See *Avaya Aura® Contact Center Commissioning* (NN44400-312).
- Install an SMTP Server. See *Avaya Aura® Contact Center Installation* (NN44400-311).

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 e-mail 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. Click **Start** > **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 e-mail 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 iceAdmin, or 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**.

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. In the **User Name,** type a name.
8. In the **Organization**, type your company name.
9. Select one of the following options:
   - Anyone who uses this computer (all users)
   - Only for me (User Name)
10. Click **Next**.
11. Accept the default Destination Folder.

    OR

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

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

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

Procedure job aid

Information about the Orchestration Designer is found in *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (NN44400-510).

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 Aura® 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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Agent Desktop Displays** > **Server Configuration Parameters**.
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 159.
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

Name	Description
	administrator for acceptable IP multicast addresses for your specific network.
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. If you leave this box empty, the system uses the default value of 1 000 agents. The maximum value that you can type in this box is 3000 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 Manager Administration 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 services.
- Reset Internet Information Services (IIS) (using the **`iisreset`** command) on the Contact Center Manager Administration server.

About this task

After you install Contact Center Manager Administration and specify a custom password for the iceAdmin user account, change the account password.

If you forget or misplace the iceAdmin password, you must reset it. For information, see Resetting the iceAdmin password on page 589.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **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 161.
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 Contact Center Manager Administration.

Configuring the LPR port for printers

Before you begin

- Ensure that you have the Windows Server 2008 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 on the CCMA server

Before you begin

- Ensure that you have administrator privileges on the Contact Center Manager Administration server.
- Configure a network printer.

- Know the computer name of the server to which the printer is attached.
- Know the share name of the printer.

About this task

Print on-demand and scheduled historical reports and scripts to a network printer. Configure a Line Print Terminal (LPT) port on the Contact Center Manager Administration server to use the network printer, and then add a local printer on this same LPT port on the Contact Center Manager Administration server.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Click **Start** > **Run**.
3. In the **Open** box, type `cmd` to open an MS-DOS prompt.
4. Click **OK**.
5. At the prompt, enter
   ```
   net use <port> [\\<print server name>\<printer share name>] /
   USER:<print server name>\Administrator /PERSISTENT:YES
   ```
   A message appears indicating that the password for the printer is invalid and asking you to type the password.
6. At the prompt, type the administrator password for the server to which the printer is attached.
7. Press **Enter**.
8. On the server, click **Start** > **Devices and Printers**.
9. In the **Devices and Printers** dialog box, select the **Add a printer** button.
10. In the **Add printer** dialog box, select **Add a local printer**.
11. Click **Next**.
12. In the **Choose a printer port** dialog box, select the **Use the following port** option.
13. From the list, select the port you typed in step 5 on page 163.
14. Deselect the **Query the printer and automatically select the driver to use** check box.
15. Click **Next**.
    The Detecting TCP/IP port window appears.
16. In the **Install the printer driver** dialog box, select the printer from the available list.
17. Optional: Click **Window Update** to view more information about the printer model.
18. Optional: Click **Have Disk** to install the printer driver from an installation disk.

19. Click **Next**.
20. In the **Which version of the driver do you want to use?** dialog box, select the **Use the driver that is currently installed (recommended)** option.
21. Click **Next**.
    The Type a printer name window with the appropriate printer name appears.
22. Click **Next**.
23. In the **Printer Sharing** dialog box, select **Do not share this printer**.
24. Click **Next**.
25. Select the **Set as the default printer** option.
26. Optional: Click **Print a test page** to check if the printer is working properly.
27. Click **Finish**.

Variable definitions

Name	Description
port	The port name.
print server name	The name of the printer server.
printer share name	The printer share name.

Configuring a network printer to use the CCMA server as the print server

Before you begin

- Ensure that you have administrator privileges on the Contact Center Manager Administration server.
- Ensure that your network printer has standard TCP/IP protocol or uses a Hewlett-Packard Jet Direct card.

About this task

Configure a network printer that uses the Contact Center Manager Administration server as the print server.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Click **Start** > **Devices and Printers**.
3. In the **Devices and Printers** dialog box, select the **Add a printer** button.
4. In the **Add printer** dialog box, select **Add a local printer**.
5. Click **Next**.
6. In the **Choose a printer port** dialog box, select the **Use an existing port** option.
7. In the **Use an existing port** drop-down list, select **LPT1: (Printer Port)**.
8. Click **Next**.
   The Detecting TCP/IP port window appears.
9. In the **Install the printer driver** dialog box, select the printer from the available list.
10. Optional: Click **Window Update** to view more information about the printer model.
11. Optional: Click **Have Disk** to install the printer driver from an installation disk.
12. Click **Next**.
    The Type a printer name window with the appropriate printer name appears.
13. Click **Next**.
14. In the **Printer Sharing** dialog box, select **Do not share this printer**.
15. Click **Next**.
16. Select the **Set as the default printer** option.
17. Optional: Click **Print a test page** to check if the printer is working properly.
18. Click **Finish**.

Configuring a network printer to use a print server other than the CCMA server

Before you begin

- Ensure that you have administrator privileges on the Contact Center Manager Administration server.
- If the print server is a UNIX computer, install Print Services for UNIX on the Contact Center Manager Administration server. To install this utility, use the Windows Server 2008 64-bit Release 2 DVD.

About this task

Configure a default network printer that is connected to a print server other than the Contact Center Manager Administration server (for example, a UNIX server).

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Click **Start** > **Devices and Printers**.
3. In the **Devices and Printers** dialog box, select the **Add a printer** button.
4. In the **Add printer** dialog box, select **Add a local printer**.
5. Click **Next**.
6. In the **Choose a printer port** dialog box, select the **Create a new port** option.
7. In the **Type of port** drop-down list, select **Standard TCP/IP Port**.
8. In the **Type a printer hostname or IP address** dialog box, type the hostname or IP address of the printer in the **Hostname or IP address** box.
   The Port Name box gets automatically populated.
9. Deselect the **Query the printer and automatically select the driver to use** check box.
10. Click **Next**.
    The Detecting TCP/IP port window appears.
11. In the **Install the printer driver** dialog box, select the printer from the available list.
12. Optional: Click **Window Update** to view more information about the printer model.
13. Optional: Click **Have Disk** to install the printer driver from an installation disk.
14. Click **Next**.

15. In the **Which version of the driver do you want to use?** dialog box, select the **Use the driver that is currently installed (recommended)** option.
16. Click **Next**.
    The Type a printer name window with the appropriate printer name appears.
17. Click **Next**.
18. In the **Printer Sharing** dialog box, select **Do not share this printer**.
19. Click **Next**.
20. Select the **Set as the default printer** option.
21. Optional: Click **Print a test page** to check if the printer is working properly.
22. Click **Finish**.

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 Configuration – Avaya CS 1000 Integration* (NN44400-512).

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 may 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 Configuration – Avaya CS 1000 Integration* (NN44400-512).

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 LandingPad.
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.

Enabling the Avaya Aura® Call Center Elite environment in Avaya Aura® Agent Desktop

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

You can enable the Avaya Aura® Call Center Elite environment in Avaya Aura® Agent Desktop, to manage both Voice contacts from Avaya Aura® Call Center Elite and Multimedia contacts from Contact Center Multimedia.

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 Multimedia server on which you want to enable the Avaya Aura® Call Center Elite environment.
4. Click **Edit Properties**.
   The system displays the Contact Center Multimedia server properties in the right pane.
5. Select the **Elite Environment** check box.

6. Click **Submit**.

Chapter 18: 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

- Connect to Avaya Communication Server 1000.

Navigation

- Extracting data from a serial connection on page 174
- Extracting data using a modem on page 175

- Extracting data from a file on page 177
- Capturing Terminal Number data on page 178
- Capturing voice port data on page 179
- Capturing CDN data on page 180
- Capturing IVR ACD-DN data on page 181
- Capturing route data on page 182

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. Click **Start** > **All Programs** > **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. Click **Start** > **Programs** > **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. Click **Start** > **Programs** > **Contact Center** > **CS1000 Data Extraction Tool** > **CS 1000 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 **DES** prompt, enter the description.
6. 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 19: Active Directory Lightweight Directory Services replication

Active Directory Lightweight Directory Services (AD-LDS) is a light-weight implementation of Active Directory and does not require the creation of domains or domain controllers. AD-LDS provides a hierarchical data store for directory data with an LDAP interface. In Windows Server 2008, Active Directory Application Mode (ADAM) has been renamed Active Directory Lightweight Directory Services (AD-LDS).

Replication means that you share the data stored in one AD-LDS instance with another AD-LDS instance, to ensure that the replicated data is the same across both servers. If the active Contact Center Manager Administration server fails, a replicating server provides immediate access to all data files stored in AD-LDS from the primary server. Contact Center Manager Administration users can use replication to immediately point their browser to the standby Contact Center Manager Administration server to maintain a level of productivity with minimal interruption of access to the Contact Center Manager Administration application.

While you may have access to multiple AD-LDS instances and multiple Contact Center Manager Administration-specific AD-LDS instances, each Contact Center Manager Administration server can have only one Contact Center Manager Administration-specific AD-LDS instance. To maintain the integrity of your Contact Center Manager Administration data, you can replicate a Contact Center Manager Administration-specific AD-LDS instance only with one or more other Contact Center Manager Administration-specific instances of AD-LDS.

AD-LDS replication is not a replacement for scheduling regular backups of your Contact Center Manager Administration data. For the following reasons, you must still schedule backups on your primary server even if you have a standby server installed with replication enabled:

- Not all Contact Center Manager Administration data files are replicated.
- You cannot use replication to roll back data to a specific point in time, which may be required.

For more information about AD-LDS, see the Microsoft Web site at www.microsoft.com.

To monitor Active Directory replication issues, you can use the Active Directory Replication Monitor (ReplMon.exe). The Active Directory Replication Monitor is a graphical user interface tool that is included with Windows Server 2008 Release 2 Support Tools. You can use the Active Directory Replication Monitor to view the status of Active Directory replication, verify replication topology, force synchronization between domain controllers, and monitor the status and performance of domain controller replication.

Navigation

- Setting up AD-LDS replication on page 184
- Choosing AD-LDS service accounts on page 186
- Stopping replication on replicating servers on page 187
- Starting replication on replicating servers on page 187

Setting up AD-LDS replication

Before you begin

- Ensure that you enable replication during the install. You cannot enable replication after you install AD-LDS.
- Ensure that you install only one instance of AD-LDS on a Contact Center Manager Administration server.
- Ensure that you install both instances of Contact Center Manager Administration before you point a Contact Center Manager Administration server AD-LDS instance to another Contact Center Manager Administration server AD-LDS instance.
- Ensure that you point the secondary server AD-LDS instance to the primary server AD-LDS instance during the install of the secondary server; you cannot do this after you install the secondary server.
- Ensure that you do not install AD-LDS on a server that is a domain controller.
- Before you install the first instance of AD-LDS with replication, ensure that you note the environment into which you install it.
- Before you replicate an existing instance of AD-LDS, ensure that you note both the environment into which you install the replica instance and the type of service account chosen for the original instance. Your choices for the replica instance depend on the Windows domain into which the original AD-LDS was installed, and on the service account chosen for the original AD-LDS instance.

About this task

You can set up AD-LDS replication so that if the active Contact Center Manager Administration server fails, a replicating server can provide immediate access to all data files stored in AD-LDS from the primary server.

Procedure

1. Install the Contact Center Manager Administration server software on the primary server without replication.

2. On the secondary server, log on to the domain as the administrator or as a user with administrative privileges.
3. On the secondary server, install the Contact Center Manager Administration server software with replication.
4. While you install the Contact Center Manager Administration server software with replication on the secondary server, point the secondary server AD-LDS instance to the primary server AD-LDS instance.

Procedure job aid

If you replicate AD-LDS during your Contact Center Manager Administration installation, only certain Contact Center Manager Administration data files are copied between replicated servers.

The following list of information is exchanged between servers, so that if it changes on one server, it is replicated to the other servers within the same domain:

- access classes
- partitions
- private and graphical real-time reports
- real-time report filters

However, not all Contact Center Manager Administration data is stored in AD-LDS, and therefore cannot be replicated. If a server fails, you must use backup files to restore the following files to the standby server, because the data is not replicated using AD-LDS:

- scheduling data for Contact Center Management assignments
- scheduling data for historical reports
- historical report output files
- user-created historical reports that are imported into Contact Center Manager Administration
- real-time report exported files
- Emergency Help exported files
- Report Creation Wizard user-created formulas (stored in the file RCW.mdb)
- Report Creation Wizard user-created reports and report definitions

Choosing AD-LDS service accounts

Before you begin

- Know the Windows workgroup or domain environment into which you installed AD-LDS.
- Know the service account chosen for the original instance of AD-LDS, if you are replicating an existing instance of AD-LDS.

About this task

Choose a service account after you install AD-LDS on the Contact Center Manager Administration server, because AD-LDS runs as a service. The type of AD-LDS service account that you can choose during the AD-LDS installation depends on the Windows workgroup or domain environment into which you install AD-LDS, and whether this is the first instance that you install on your network or if you replicate an existing instance.

By default, AD-LDS is always installed as a network service account, unless you manually change the service account settings to domain user or workstation user.

Procedure

After you install AD-LDS, and based on the environment into which you installed AD-LDS, choose the appropriate AD-LDS service account.

Procedure job aid

Table 2: AD-LDS service account options

Domain context	Service account (primary server)	Service account (secondary server)	Default replication authentication method
Windows Server 2000 domain OR Windows Server 2008 Release 2 domain or forest	Network service	Network service or Domain user	Negotiated
	Workstation user	Workstation user	Negotiated pass-through
	Domain user	Network service or Domain user	Negotiated

Stopping replication on replicating servers

About this task

Stop AD-LDS replication on all replicating servers.

Procedure

1. Click **Start** > **Run**.
2. In the text box, type `cmd`.
3. Click **OK**.
4. Navigate to the ADAM directory, for example, C:\Windows\ADAM.
5. To disable outbound replication, type `repadmin /options localhost:389 +DISABLE_OUTBOUND_REPL`.
6. Press `Enter`.
7. Close all windows.

Starting replication on replicating servers

About this task

Start AD-LDS replication on all replicating servers.

Procedure

1. Click **Start** > **Run**.
2. In the text box, type `cmd`.
3. Click **OK**.
4. Navigate to the ADAM directory, for example, C:\Windows\ADAM.
5. To enable outbound replication, type `repadmin /options localhost:389 -DISABLE_OUTBOUND_REPL`.
6. Press `Enter`.
7. Close all windows.

Chapter 20: Contact Center Manager Administration failure recovery

If the Contact Center Manager Administration server hardware fails, you must restore your backup data quickly.

Prerequisites for Contact Center Manager Administration server failure recovery

- Ensure that you restore data that was backed up from the same release and version of the software as that which is currently installed on the Contact Center Manager Administration server.
- Do not attempt to restore data from previous Service Packs. If you restore data backed up on previous versions, you corrupt your server.

Contact Center Manager Administration server failure recovery procedures

About this task

This task flow shows you the sequence of procedures you perform to recover from Contact Center Manager Administration server failure, both with and without a replicating server installed.

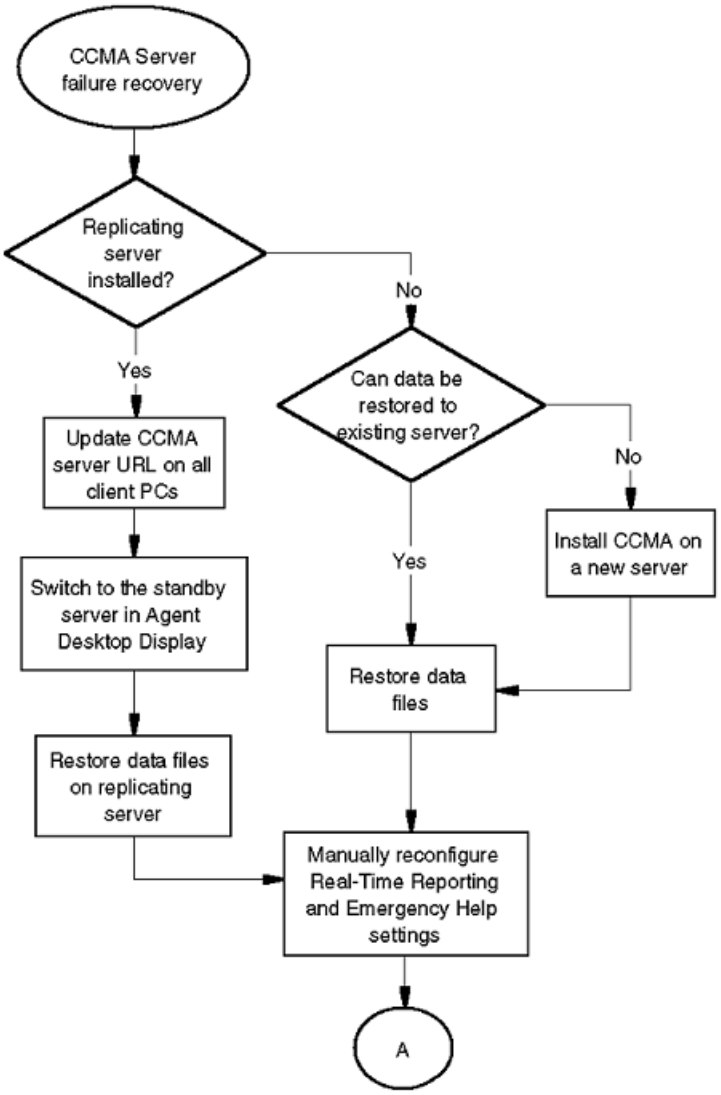


Figure 1: Contact Center Manager Administration server failure recovery procedures

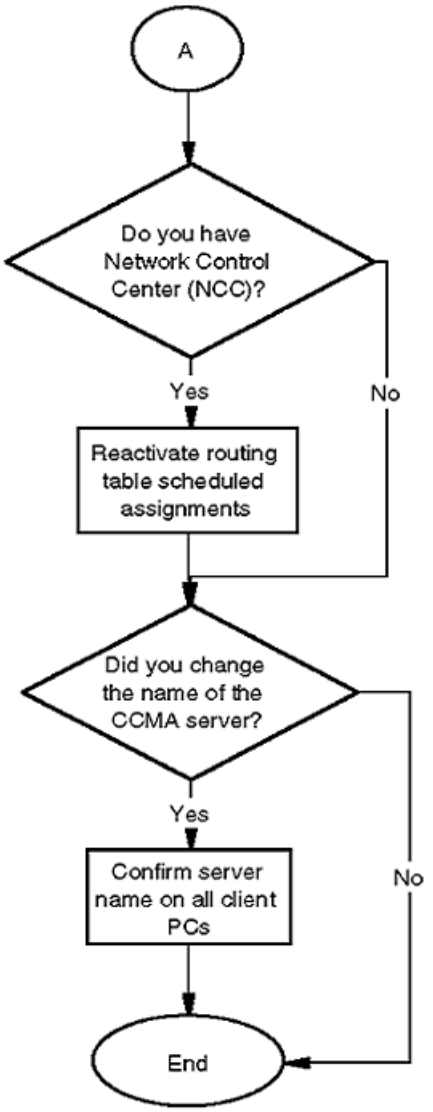


Figure 2: Contact Center Manager Administration server failure recovery procedures (continued)

Job aid: Functionality after CCMA server failure recovery

In a Contact Center Manager Administration server failure disaster, with replication enabled, all information in AD-LDS is replicated to the secondary server. This enables operation of the contact center to continue.

Many functions are maintained and are immediately available from the replicating server. However, some Contact Center Manager Administration information is held in flat files or databases outside AD-LDS. To enable all features in Contact Center Manager Administration,

you must manually restore the files from ..\Avaya\Contact Center\Manager Administration to the replicating server.

Chapter 21: 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 and Contact Center Manager Administration support the following languages:

- English
- French
- German
- Japanese
- Russian
- Simplified Chinese
- Traditional Chinese
- LA Spanish
- Brazilian Portuguese
- Italian
- Korean

You can install a language pack to access translated graphical user interfaces, Historical Reporting templates, and Online Help. See the Avaya Aura® Contact Center Localization Release Notes for further information.

Navigation

- Language levels on page 194
- Language family compatibility on page 194

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 graphic 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 graphic user interface, the online Help, and all reports are translated into one of the eight 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.

In this environment, you must install the CCMA language pack on the Contact Center Manager Administration server and the CCMM language pack on the Contact Center Multimedia server. See the Avaya Aura® Contact Center Localization 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 co-resident servers compatibility, see the Avaya Aura® 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.

Chapter 22: Security Framework configuration

The Security Framework provides an identify management security framework that enables integration with the customer directory services infrastructure (for example Active Directory) for authentication and authorization of a user. The Security Framework helps reduce the administrative costs and eliminates the redundant user information associated with each application.

The procedures in this chapter are optional configuration steps to enable security certificates or to disable the Security Framework in Contact Center. Key procedures to configure the Security Framework are in *Avaya Aura® Contact Center Commissioning* (NN44400-312).

If you plan to use the Security Framework for your Contact Center, Avaya recommends that you do not use the Contact Center Manager Administration security.

Prerequisites to Security Framework configuration

- Install the Security Framework. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- Commission the Security Framework. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Configuring the Contact Center Manager Administration security details on page 198
- Disabling the Security Framework on page 199
- Saving the root certificate authority to a file on page 200
- Importing the root certificate authority to Internet Explorer on page 200
- Configuring security prompts in Internet Explorer on page 201
- Viewing the security server settings on page 202

Configuring the Contact Center Manager Administration security details

Before you begin

- Install and configure your Contact Center Manager Administration security server.

About this task

Configure the Contact Center Manager Administration security details to record the location and settings of your security server.

Procedure

1. From the **Start** menu, select **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Configuration** > **Security Settings**.
2. In the Security Details window, under **Configuration Setup**, select the option to indicate where your security server is installed.
3. In the **Contact Center Manager Administration (CCMA) Details** group, select the **Web Site Identifier** of the Contact Center Manager Administration Web site from the list.
4. Select your **CCMA Server Protocol**.
5. Select the **IIS Port Number** for the Contact Center Manager Administration server.
6. In the **Security Server Details** group, type the details of the Contact Center Manager Administration security server, including the FDQN, Protocol, and Port Number.
7. Click **Enable**.
   A confirmation message appears indicating that the CCMA Security Details configuration of the security server was successful.

Variable definitions

Name	Description
Configuration Setup	The location of the installed security server: On this server (Co-resident with CCMA) or Other Server.

Name	Description
Web Site Identifier	A list of available Web site location identifiers.
CCMA Server Protocol	The security protocol of the CCMA server: http or https.
IIS Port Number	A list of available IIS port locations. The default is the location of the Contact Center Manager Administration server.
Security Server FQDN	The Fully Qualified Domain Name (FQDN) of the Contact Center Manager Administration security server, for example, server1.Avaya.com.
Security Server Protocol	The security protocol of the Contact Center Manager Administration security server: http or https.
Security Server Port Number	The port number of the Contact Center Manager Administration security server, for example, 8443.

Disabling the Security Framework

About this task

Disable the Security Framework if you need to access the Contact Center Manager Administration server without the restriction of the security policies or to revert to the old Contact Center Manager Server log on method without the Security Framework.

Procedure

1. On the **Start** menu, click **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Configuration** > **Security Settings**.
2. In the Security Details window, click **Disable**.

Saving the root certificate authority to a file

Before you begin

- Ensure that you have a server certificate.

About this task

Save the root certificate authority to a file that is accessible to the client so that you can import the security certificate to the browser.

Procedure

1. Log on to the Unified Communication Management (UCM) utility using the Administrator account, with the **User ID** admin.
2. Under **Security**, click **Certificates**.
3. Click the **Private Certificate Authority** tab.
4. Click **Download** and then name and save the security certificate to a file.

Importing the root certificate authority to Internet Explorer

Before you begin

- Install and configure your Contact Center Manager Administration security server.
- Save the security certificate to a file. For more information, see Saving the root certificate authority to a file on page 200.

About this task

Import the root certificate authority to the browser to prevent Internet Explorer from displaying a Security Alert when you connect to the security server. You must add the Root CA certificate to Trusted Root Certification Authorities.

Procedure

1. Open Internet Explorer.
2. Select **Tools** > **Internet Options**.
3. Click the **Content** tab.
4. Click **Certificates**.
5. In the Certificates window, click the **Trusted Root Certification Authorities** tab.

6. Click **Import**.
7. In the Certificate Import Wizard, perform the steps to import the security certificate for the Contact Center Manager Administration security server. Locate and select the certificate from the location where you saved the file and accept all other defaults in the Wizard.
8. Click **Finish**.
9. Restart your browser to apply the changes.

Configuring security prompts in Internet Explorer

About this task

Configure security prompts in the Internet Explorer browser to suppress warning messages that can appear when you access the security server URL.

Procedure

1. Open Internet Explorer.
2. Select **Tools** > **Internet Options**.
3. Click the **Security** tab.
4. Click **Trusted Sites**.
5. Click **Custom Level**.
6. In the Security Settings window, scroll through the list until you find the option **Don't prompt for client certificate selection when no certificates or only one certificate exists**, and then click **Enable** for this setting.
7. Click **OK**.
8. Click **Yes** to confirm the change.
9. Click **OK**
10. Restart your browser to apply the changes.

Viewing the security server settings

Before you begin

- If you want to enforce SSL between the CCMA and SFW server, ensure that you have a certificate installed on the CCMA Web server.

About this task

Use the application to view the security framework (SFW) port settings, to enable or disable the enforcement of SSL between the Contact Center Manager Administration server and the security framework, or to restart the SFW service.

Do not change the port numbers for the SFW service.

Procedure

1. Log on to the Contact Center Manager Administration security server.
2. From the **Start** menu, select **All Programs** > **Avaya** > **Contact Center** > **Security Framework** > **Security Server Settings**.
3. In the **Security Settings** dialog box, select the **Enforce secure channel (SSL) communications** check box if you want to enforce SSL between the CCMA and SFW server.
4. Select the **Restart Security Service** check box.
5. Click **Update**.
6. Confirm changes by accepting any warning messages that appear.
7. Click **Close**.

Part IV: Security Framework

- User identity provisioning on page 205
- Role creation and management on page 209
- Element and permission mapping on page 211
- Role mapping on page 215
- Policy creation and management on page 217
- External identity repository configuration on page 221
- Element Management on page 229
- Security log management on page 233
- Account and password management on page 235
- Session management on page 241

Chapter 23: User identity provisioning

Provision user identities to supply accounts that allow you to access the Avaya Aura® Contact Center server.

Navigation

- Adding a local user identity and password on page 205
- Adding an external account (optional) on page 206

Adding a local user identity and password

About this task

Add a local user identity and password to set up an administrator who is authenticated locally in Unified Communications Management (UCM).

Procedure

1. Log on to UCM as a security administrator.
2. In the navigation pane, click **User Services** > **Administrative Users**.
3. On the **Administrative Users** page, click **Add**.
4. On the **Add New Administrative User Step 1** page, in the **User ID** field, type a user ID.
5. In the **Authentication Type** section, click **Local**.
6. In the **Full Name** field, type the full name of the user.
7. In the **Temporary password** field, type a password for the user.
8. In the **Re-enter password** field, retype the password.
9. Click **Save** and **Continue**.
10. On the **Add New Administrative User Step 2** page, select one or more **Role Name** check boxes to assign roles to the new local user.

11. Click **Finish**.

Variable definitions

Name	Description
Local	Specifies a user who is authenticated locally in Unified Communications Management (UCM).
Full Name	The full name of the user, including first and last name.
Re-enter password	Retype the temporary password.
Temporary Password	The temporary password required to connect to UCM.
User ID	A unique identifier used by an administrative user to log on to UCM. Valid values are 1 to 31 characters. Valid characters are a to z, A to Z, 0 to 9, - and _.

Adding an external account (optional)

Before you begin

- Provision an external server. For more information, see External identity repository configuration on page 221.

About this task

Add an external account to Unified Communications Management (UCM) to set up an administrator who is authenticated with external authentication. Contact Center performs external authentication through Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS), or Kerberos.

Procedure

1. Log on to UCM as a security administrator.
2. In the navigation pane, click **User Services** > **Administrative Services**.
3. On the **Administrative Users** page, click **Add**.
4. On the **Add New Administrative User Step 1** page, in the **User ID** field, type a user ID.

5. In the **Authentication Type** section, click **External**.
6. In the **Full Name** field, type the full name of the user.
7. Click **Save** and **Continue**.
8. On the **Add New Administrative User Step 2** page, select one or more **Role Name** check boxes to assign roles to the new external user.
9. Click **Finish**.

Variable definitions

Name	Description
External	Specifies a user who is authenticated externally. Contact Center performs external authentication through Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS), or Kerberos.
Full Name	The full name of the user, including first and last name.
User ID	A unique identifier used by an administrative user to log on to UCM. Valid values are 1 to 31 characters. Valid characters are a to z, A to Z, 0 to 9, - and _.

Chapter 24: Role creation and management

Create and manage roles to control user access to elements.

Navigation

- Creating a custom role on page 209
- Deleting a custom role (optional) on page 210

Creating a custom role

About this task

Create a role to control user access to elements.

You can assign roles to users. Each role defines the management functions a user can perform on an element.

Procedure

1. Log on to Unified Communications Management as a security administrator.
2. In the navigation pane, click **Security** > **Roles**.
3. On the **Roles** page, click **Add**.
4. On the **Add New Role Step 1** page, in the **Role Name** field, type a unique name for the role.
5. In the **Role Description** field, type a description for the role.
6. Click **Save** and **Continue**.
7. On the **Role Details** page, click **Save**.

Variable definitions

Name	Description
Role Description	A description of the role. The description may be up to 500 characters long. Allowed characters are a-z, A-Z, 0-9, - and _.
Role Name	A unique name for the role. The name must be at least one character long. Allowed characters are a-z, A-Z, 0-9, - and _.

Deleting a custom role (optional)

Before you begin

- You must create a custom role.

About this task

Delete a role to remove custom roles from Unified Communications Management (UCM). You cannot delete built-in roles.

Procedure

1. Log on to UCM as a security administrator.
2. In the navigation pane, click **Security** > **Roles**.
3. On the **Roles** page, select the check box next to the role you want to delete.
4. Click **Delete**.
5. On the **Delete Roles** page, click **Delete**.

Chapter 25: Element and permission mapping

Map element permissions to a role to control which management functions a user with that role can perform on an element.

Navigation

- Mapping elements and permissions to a role on page 211
- Mapping elements and permissions by copying from another role on page 212
- Removing elements from a role (optional) on page 213

Mapping elements and permissions to a role

About this task

Map elements and permissions to a role to control which management functions a user with that role can perform on an element.

Procedure

1. Log on to UCM as a security administrator.
2. In the navigation pane, click **Security** > **Roles**.
3. On the **Roles** page, in the **Role Name** column, click the name of the role to which you want to map elements.
4. On the **Role Details** page, on the **Element/Service Permission** tab, select the check boxes next to the elements for which you want to map permissions.
5. Click **Add Mapping**.
6. On the **Select Element and/or Network Service To Map to Role** page, in the **Group Name** list, select the group you want to map to the role.
7. On the **Select Element and/or Network Service To Map to Role** page, in the **Element and/or Network Service Name** list, select the element you want to map to the role.

8. Click **Next**.
9. On the **Permission Mapping** page, in the **Template for permission setting set** list, select a permission setting template.
10. Optionally, select the **Allow access to Contact Center** or the **Allow access to hyperlinks** check box, if applicable.
11. Click **Save**.

Variable definitions

Name	Description
Allow use of Element Manager	Select this check box to allow users with this role to use Element Manager.

Mapping elements and permissions by copying from another role

About this task

Copy element and permissions mapping from another role to assign the same access as an existing role.

Procedure

1. Log on to UCM as a security administrator.
2. In the navigation pane, click **Security** > **Roles**.
3. On the **Roles** page, in the **Role Name** column, click the name of the role to which you want to map elements.
4. On the **Role Details** page, on the **Element/Service Permission** tab, select the check boxes next to the elements for which you want to map permissions.
5. Click **Copy All From**.
6. On the **Permission Mapping** page, in the **Copy from Role** list, select the role from which you want to copy permissions.
7. Click **Copy**.

Removing elements from a role (optional)

About this task

Remove elements from a role to remove access to that element for users with that role.

Procedure

1. Log on to UCM as a security administrator.
2. In the navigation pane, click **Security** > **Roles**.
3. On the **Roles** page, in the **Role Name** column, click the name of the role to which you want to map elements.
4. On the **Role Details** page, on the **Element/Service Permission** tab, select the check boxes next to the elements for which you want to map permissions.
5. Click **Delete Mapping**.
6. On the **Delete Mapping** page, click **Delete**.

Chapter 26: Role mapping

Map roles and users to grant users the element permissions associated with a selected role.

Navigation

- Assigning roles to a user on page 215
- Assigning users to a role on page 216

Assigning roles to a user

About this task

Assign roles to a user to grant the user the element permissions associated with selected roles.

You can also assign roles to a user by copying them from another role. For information, see Mapping elements and permissions by copying from another role on page 212.

Procedure

1. Log on to UCM as a security administrator.
2. In the navigation pane, click **User Services** > **Administrative Users**.
3. On the **Administrative Users** page, click the User ID of the user for whom you want to assign a role.
4. On the **User Details** page, in the **Roles** pane, click **Select Roles**.
5. On the **User Roles** page, select the check boxes next to the roles that you want to assign to the user.
6. Click **Save**.

Assigning users to a role

About this task

Assign users to a role to grant users the element permissions associated with a selected role.

Procedure

1. Log on to UCM as a security administrator.
2. In the navigation pane, click **Security** > **Policies**.
3. On the **Roles** page, in the **Role Name** column, click the name of the role to which you want to assign users.
4. On the **Role Details** page, select the **Assigned Users** tab.
   The Role Details page refreshes with a list of users who are granted the permissions associated with the selected role.
5. Click **Select Users**.
6. On the **Assigned Users** page, select the check boxes next to the users for whom you want to add the permissions associated with the selected role.
7. Click **Save**.

Chapter 27: Policy creation and management

Create and manage policies to enforce rules that help ensure security. In Unified Communications Management (UCM), security policies apply to passwords and session management.

Navigation

- Creating a security policy for passwords on page 217

Creating a security policy for passwords

About this task

Create a security policy for passwords to configure aging, history, strength, and lockout parameters for passwords used for locally authenticated users in UCM. Set your password policies according to your business requirements.

Procedure

1. Log on to Unified Communications Management as an administrator.
2. In the navigation pane, click **Security** > **Policies**.
3. On the **Policies** page, in the **Password Policy (for locally authenticated users)** pane, click **Edit**.
4. On the **Password Policy** page, select the **Aging** check box.
5. In the **Expiration period** field, type the number of maximum allowable days before the password expires.
6. In the **Expiration warning** field, type the number of days before a password expires to send a warning to a user.
7. In the **Minimum age** field, type the minimum allowable days for a password age.
8. Select the **History** check box.
9. In the **Previous passwords blocked** field, type the number of passwords to remember in history.

10. In the **Strength** section, in the **Minimum Total Length** field, type the minimum number of characters required for a password.
11. In the **Minimum by character Type** section, in the **Lower case** field, type the minimum number of lower case characters required for a password.
12. In the **Upper case** field, type the minimum number of upper case characters required for a password.
13. In the **Numeric case** field, type the minimum number of numeric characters required for a password.
14. In the **Special case** field, type the minimum number of special characters required for a password.
15. Select the **Lockout** check box.
16. In the **Consecutive Invalid Login Attempts** field, type the maximum number of failed logon attempts before the system locks out a user.
17. In the **Interval for Consecutive Invalid Login Attempts** field, type the number of seconds allowed for consecutive invalid logon attempts before the system locks out the user.
18. In the **Lockout Time** field, type the number of minutes an account can remain unused before the system locks it.
19. Click **Save**.

Variable definitions

Name	Description
Consecutive Invalid Login Attempts	The maximum number of failed logon attempts before the system locks out a user. The maximum number of failed login attempts must be at least one.
Expiration period	The number of maximum allowable days before the password expires. Valid values are 1 to 365 days. The user is forced to change the password after the threshold for the password expires and before the threshold to disable the account. The password is locked until it is reset by the security administrator.
Expiration warning	The number of days before a password expires to send a warning to a user. Valid values are 1 to 15 days. The user receives a

Name	Description
	password expiration warning when the password is about to expire and before the password expires.
Interval for Consecutive Invalid Login Attempts	The number of minutes allowed for consecutive invalid logon attempts before the system locks out the user. Valid values are 0 or more minutes.
Lockout Time	The number of minutes an account can remain unused before the system locks it. Valid values are 0 or more minutes.
Lower case	The minimum number of lower case characters required for a password. The minimum number of lower case characters cannot exceed the minimum total length. Enter a value of 0 to indicate that passwords do not require a minimum number of lower case characters.
Minimum age	The minimum allowable days for a password age. A minimum age prevents password recycling that otherwise defeats the history policy. Valid values are 0 to 7 days. The new password of the user is rejected when the current password has not reached the minimum password duration.
Minimum Total Length	The minimum number of characters required for a password. The minimum total length must be at least 6 characters.
Numeric case	The minimum number of numeric case characters required for a password. The minimum number of numeric case characters cannot exceed the minimum total length. Enter a value of 0 to indicate that passwords do not require a minimum number of numeric case characters.
Previous passwords blocked	The number of passwords to remember in history. Valid values are 1 to 99 previous passwords.
Special case	The minimum number of special case characters required for a password. An example of a special character is an exclamation mark (!). The minimum number of special case characters cannot exceed the minimum total length. Enter a value of 0 to indicate that passwords do not require a

Name	Description
	minimum number of special case characters.
Upper case	The minimum number of upper case characters required for a password. The minimum number of upper case characters cannot exceed the minimum total length. Enter a value of 0 to indicate that passwords do not require a minimum number of upper case characters.

Chapter 28: External identity repository configuration

Configure external identity repositories to enable external authentication for Contact Center.

External identity repository configuration procedures

About this task

The following task flow shows the order of procedures you perform to configure external identity repositories on Unified Communications Management (UCM). To link to any procedure, go to External identity repository configuration navigation on page 222.

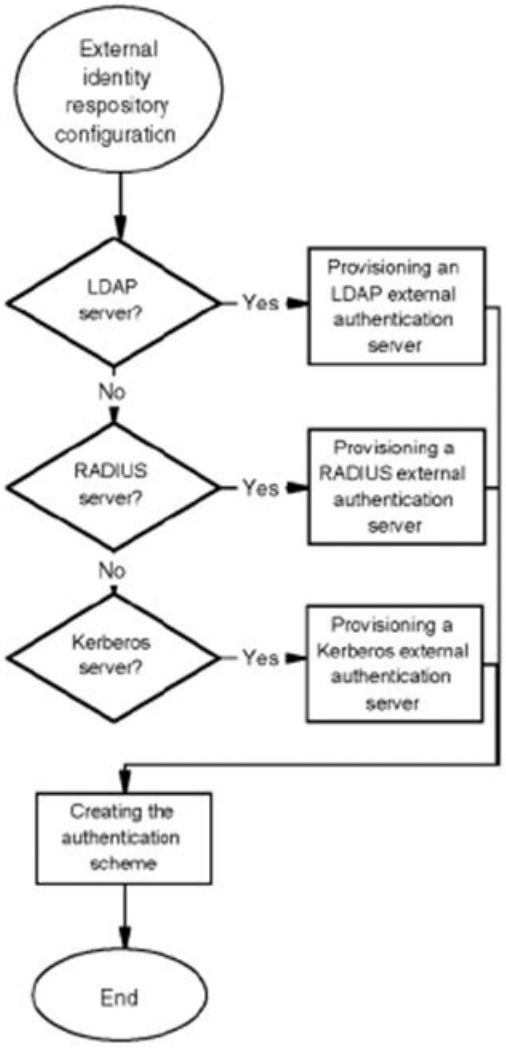


Figure 3: External identity repository configuration procedures

External identity repository configuration navigation

About this task

- Provisioning an LDAP external authentication server on page 223
- Provisioning a RADIUS external authentication server on page 224
- Provisioning a Kerberos external authentication server on page 225
- Creating the authentication scheme on page 227

Important:

Support for Security Framework fail-over is not available for Kerberos and RADIUS authentication.

Provisioning an LDAP external authentication server

About this task

Provision a Lightweight Directory Access Protocol (LDAP) authentication server to enable external authentication for Contact Center LDAP.

Procedure

1. Log on to Unified Communications Management as a security administrator.
2. In the navigation pane, click **User Services** > **External Authentication**.
3. On the **External Identity Repositories** page, in the **Authentication Servers** pane, click **Configure**.
4. On the **Authentication Servers** page, select the **Provision LDAP Server** check box.
5. In the **Provision LDAP Server** pane, in the **IP (or DNS)** field, type the IP or DNS for the server.
6. In the **TCP Port** field, type the TCP port.
7. In the **Base Distinguished Name** field, type the base distinguished name.
8. Optionally, select the **SSL/TLS Mode** check box.
9. Optionally, select the **Is Active Directory** check box.
10. In the **Distinguished Name for Root Binding** field, type a distinguished name for root binding.
11. In the **Password for Root Binding** field, type a password.
12. Click **Save**.

Important:

After you provision an LDAP authentication server, an external user account is automatically added. This new user account is based on the information you typed in the Distinguished Name for Root Binding field, which refers to a pre-existing Windows log on account.

Variable definitions

Name	Description
Base Distinguished Name	Path of the root node in the directory server from which the system can start searching for users.
Distinguished Name for Root Binding	Path of the node in the directory server pointing to a user with administrator rights. This node binds to the LDAP server during the authentication process.
IP (or DNS)	IP address or DNS of the LDAP server.
Is Active Directory	Select this check box if the LDAP server is a Windows server with Active Directory installed on it.
Password for Root Binding	The password of the administrative user who is identified through the distinguished name for root binding field.
SSL/TLS Mode	Select this check box if the communication is carried out through a secure protocol like SSL.
TCP Port	Port for network communication with the LDAP server; the standard port is 389, but 3268 may also be used in the context of the global catalog.

Provisioning a RADIUS external authentication server

About this task

Provision a Remote Authentication Dial In User Service (RADIUS) authentication server to enable external authentication for Contact Center using RADIUS.

Procedure

1. Log on to Unified Communications Management as a security administrator.
2. In the navigation pane, click **User Services** > **External Authentication**.
3. On the **External Identity Repositories** page, in the **Authentication Servers** pane, click **Configure**.

4. On the **Authentication Servers** page, select the **Provision Radius Server** check box.
5. In the **Provision Radius Server** pane, in the **IP (or DNS)** field, type the IP or DNS for the server.
6. In the **UDP Port** field, type the UDP port number.
7. In the **Shared Secret** field, type a shared secret.
8. Click **Save**.

Variable definitions

Name	Description
IP (or DNS)	IP address or DNS of the RADIUS server.
Shared Secret	A password that is shared between the RADIUS server and clients. The administrator configures the shared secret the first time the RADIUS server is configured.
UDP Port	The port for network communication with the RADIUS server. The standard port is 1812.

Provisioning a Kerberos external authentication server

About this task

Provision a Kerberos authentication server to enable external authentication for Contact Center using the Kerberos computer network authentication protocol.

When Kerberos is configured, only SSO is enabled with the browser. Kerberos also allows you to remain authenticated if the session management values (max session or max idle time) expire. These features do not apply to Orchestration Designer (OD). In OD, if the session values expire, you must re-authenticate through Contact Center Manager Administration, and then log on to OD.

Procedure

1. Log on to Unified Communications Management as a security administrator.
2. In the navigation pane, click **User Services** > **External Authentication**.

3. On the **External Identity Repositories** page, in the **Authentication Servers** pane, click **Configure**.
4. On the **Authentication Servers** page, select the **Provision Kerberos Server** check box.
5. In the **Provision Kerberos Server** pane, in the **DC Host Name (FQDN)** field, type the fully qualified domain name (FQDN) for the Kerberos server.
6. In the **DC Computer Domain** field, type the domain name of the Kerberos server.
7. In the **Keytab File** field, type the absolute path of the keytab file on the UCM server.

   OR

   Click **Browse** to browse to the keytab file on the UCM server.
8. Click **Save**.

Variable definitions

Name	Description
DC Computer Domain	The domain name of the Kerberos server. For example, tommy1.tommy.net. A Kerberos server is a Domain Controller machine implementing the Kerberos authentication protocol. A Domain Controller machine (DC) is a Windows 2008 Release 2 server with an Active Directory (AD) installed on it, that is some form of repository containing information about miscellaneous entities on the network, such as user accounts or printers.
DC Host Name (FQDN)	The fully qualified domain name for the Kerberos server. For example, CCMATMDEV2tommy1.tommy.net.
Keytab File	An encrypted copy of the Kerberos server's key. This file is generated on the Kerberos server and then copied to the UCM server.

Creating the authentication scheme

Before you begin

- Configure at least one external authentication server.

About this task

Create an authentication scheme to define the order of the authentication servers that the Contact Center uses to authenticate users.

Procedure

1. Log on to Unified Communications Management as a security administrator.
2. In the navigation pane, click **User Services** > **External Authentication**.
3. On the **External Identity Repositories** page, in the **Authentication Scheme** pane, click **Edit**.
4. On the **Authentication Scheme** page, select the option that represents the order of the authentication servers that the Contact Center uses to authenticate users.

   Important:

   The number of options on the Authentication Scheme page depends on the number of external authentication servers in your system.
5. Click **Save**.

Chapter 29: Element Management

If you are authenticated locally in Unified Communications Management (UCM), you must follow the following procedures to manage elements in the UCM application.

The following procedures are optional if you are authenticated through the Security Framework.

Navigation

- Adding a new Contact Center application (optional) on page 229
- Editing a secured element (optional) on page 230
- Deleting a secured element (optional) on page 231

Adding a new Contact Center application (optional)

Before you begin

- Ensure you obtain the Uniform Resource Locator (URL) of the server.

About this task

Add a new application to allow UCM to control which users can access an application.

Procedure

1. Log on to Unified Communications Management as a security administrator.
2. In the navigation pane, choose **Network** > **Elements**.
3. On the **Elements** page, click **Add**.
4. On the **Add New Element Step 1** page, in the **Name** field, type a name for the element.
5. Optionally, in the **Description** field, type a description for the element.
6. In the **Type** list, select **Contact Center** or **Hyperlink**.

Important:

The **Type** list is dynamic, based on the type of elements in your system. Depending on your system configuration, you may see options in addition to the Contact Center option.

7. Click **Next**.
8. On the **Add New Element Step 2** page, in the **Server Address** field, type the **URL** of the server.
9. Click **Save**.

Variable definitions

Name	Description
Description	A description for the element.
Name	A unique identifier for the element. The name can include 1 to 32 characters in length.
Release	The software release of the new element.
Server Address	The IP address and port of the new element. Use the following format: https://<FQDN of Avaya Media Server>:8443

Editing a secured element (optional)

Before you begin

- Add an element. For more information, see Adding a new Contact Center application (optional) on page 229.

About this task

Edit an element to change the properties and role-permission mapping.

Procedure

1. Log on to Unified Communications Management as a security administrator.
2. In the navigation pane, click **Network** > **Elements**.
3. On the **Elements** page, select the check box next to the element that you want to edit.

4. Click **Edit**.
5. On the **Element Details** page, make the required changes. For more information about a field, click the **Help** link in the top right of the **Element Manager** page to access the online **Help**.
6. Click **Save**.

Deleting a secured element (optional)

Before you begin

- Add an application. For more information, see Adding a new Contact Center application (optional) on page 229.

Important:

If you cannot add new elements or delete selected elements after you restart the security service, click the Refresh icon on the Elements page.

About this task

Remove an element from UCM if you no longer require the element.

Procedure

1. Log on to UCM as a security administrator.
2. In the navigation pane, click **Network** > **Elements**.
3. On the **Elements** page, select the check boxes next to the elements that you want to delete.
4. Click **Delete**.
5. On the **Delete Elements** page, click **Delete**.

Important:

UCM maintains an in-memory cache for all elements accessed from the current Web server. After you delete an element, the in-memory cache still contains the information for the element. However, UCM denies all permissions on an element after you delete it.

Chapter 30: Security log management

Manage security logs to track security information for your elements. Log files can be opened directly, or downloaded for offline analysis.

Navigation

- Inspecting security logs on page 233
- Downloading and inspecting security logs on page 233
- Reloading data from the UCM backup on page 234

Inspecting security logs

About this task

Inspect security logs to open and view management activity information for all servers in your Unified Communications Management framework.

Procedure

1. Log on to Unified Communications Management as a security administrator.
2. In the navigation pane, click **Tools** > **Logs**.
3. On the **Logs** page, in the **Filename** column, click the name of the log you want to view.

Downloading and inspecting security logs

About this task

Download and inspect security logs to download and view management activity information for all servers in your UCM framework on your local system.

Procedure

1. Log on to Unified Communications Management as a security administrator.
2. In the navigation pane, click **Tools** > **Logs**.
3. On the **Logs** page, in the **Filename** column, right-click the name of the log you want to download, and select **Save Target As** in the shortcut menu.
4. In the **Save As** window, browse to where you want to save your log file and click **Save**.
5. In the **Download Complete** window, click **Close**.
6. Click the Windows **Start** button.
7. Click **My Computer**.
8. Browse to where you saved your log file, and double-click the file to open the file and view the contents.

Reloading data from the UCM backup

About this task

Use the Data tool to reload data from the UCM backup. Reloading data deletes data from the current server and reloads data from the peer server. It terminates all active UCM sessions and restarts the UCM web server.

Procedure

1. Log on to Unified Communications Management as a security administrator.
2. In the navigation pane, click **Tools** > **Data**.
3. On the **Data Tools** page, click the **Reload from UCM Backup** button to reload data from the UCM backup.

Chapter 31: Account and password management

Manage user accounts and passwords to control who can access your Contact Center server.

Navigation

- Changing your password on page 235
- Resetting a user password on page 236
- Disabling a user account (optional) on page 237
- Reenabling a user account (optional) on page 238
- Deleting a user account (optional) on page 238

Changing your password

About this task

Change your password to ensure the security of an admin account.

You can only configure Unified Communication Management (UCM) users on the primary security server. If your system security is managed by the backup Security Framework server, then you cannot make any changes to a user account.

Important:

You must wait 24 hours after setting a password before the system allows you to change it again.

Procedure

1. Log on to Unified Communications Management (UCM) as a security administrator, using the account for which you want to change the password.
2. In the navigation pane, click **User Services** > **Password**.
3. Click **Change Password**.

4. On the **Change Password** page, in the **Current password** field, type your current password.
5. In the **New password** field, type your new password.
6. In the **Confirm new password** field, retype your new password.
7. Click **Save**.

Variable definitions

Name	Description
New password	The new password for the administrator account. Allowed characters in the password are: { } | ( ) , / . = [ ] ^ ~ _ @ ! ‘ ; a-z A-Z and 0-9. The new password must conform to any password policies defined by the security administrator. Applicable password policies are listed at the bottom of the Change Password page.

Resetting a user password

Before you begin

- Ensure that the user for whom you want to reset the password is locally authenticated. You cannot reset the password for an externally authenticated user.

About this task

Reset user passwords when users cannot remember their password.

You can only configure Unified Communication Management (UCM) users on the primary security server. If your system security is managed by the backup Security Framework server, then you cannot make any changes to a user account.

Procedure

1. Log on to Unified Communications Management (UCM) as a security administrator.
2. In the navigation pane, click **User Services** > **Administrative Users**.
3. On the **Administrative Users** page, in the **User ID** column, click the link of the user whose password you want to reset.

4. On the **User Details** page, in the **Password** field, type a new password for the user.
5. In the **Re-enter password** field, retype the new password.
6. Click **Save**.

   The next time the user logs on, UCM prompts the user to change the password.

Variable definitions

Name	Description
Password	The password used to log on to ECM. Allowed characters in the password are: { } | ( ) , / . = [ ] ^ ~ _ @ ! ‘ ; a-z A-Z and 0-9. The password is a minimum of eight characters long.

Disabling a user account (optional)

About this task

Disable a user account if the user no longer requires access.

You can only configure Unified Communication Management (UCM) users on the primary security server. If your system security is managed by the backup Security Framework server, then you cannot make any changes to a user account.

Procedure

1. Log on to Unified Communications Management as a security administrator.
2. In the navigation pane, click **User Services** > **Administrative Users**.
3. On the **Administrative Users** page, select the check box next to the user you want to disable.
4. Click **Disable**.

Reenabling a user account (optional)

About this task

Reenable a user account to grant access again to a user whose account is disabled.

You can only configure Unified Communication Management (UCM) users on the primary security server. If your system security is managed by the backup Security Framework server, then you cannot make any changes to a user account.

Procedure

1. Log on to Unified Communications Management as a security administrator.
2. In the navigation pane, click **User Services** > **Administrative Users**.
3. On the **Administrative Users** page, in the **User ID** column, click the link for the disabled account.

   If the user is disabled, **Disabled** appears in the **Status** column.
4. On the **User Details** page, select **Enabled**.
5. Click **Save**.

Deleting a user account (optional)

About this task

Delete a user account to remove a user from the system.

You can only configure Unified Communication Management (UCM) users on the primary security server. If your system security is managed by the backup Security Framework server, then you cannot make any changes to a user account.

Procedure

1. Log on to Unified Communications Management as a security administrator.
2. In the navigation pane, click **User Services** > **Administrative Users**.
3. On the **Administrative Users** page, select the check box next to the user account you want to delete.

   You can select multiple users to delete more than one account at a time.
4. Click **Delete**.

5. On the **Delete Users** page, click **Delete**.

Chapter 32: Session management

Manage active sessions to ensure that only authorized administrators are logged on to Unified Communications Management (UCM).

Navigation

- Viewing active sessions on page 241
- Ending sessions manually on page 241

Viewing active sessions

About this task

View active sessions to determine who is logged on to UCM as an administrator.

Procedure

1. Log on to Unified Communications Management as a security administrator.
2. In the navigation pane, click **Security** > **Active Sessions**.

Ending sessions manually

About this task

End sessions manually to stop sessions that are initiated by unauthorized users.

Procedure

1. On the **Active Sessions** page, in the **User ID** column, select the check box next to the user for whom you want to end a session.
2. Click **Terminate**.

Part V: Network Control Center Server

- Networking Service Monitor configuration on page 245
- Network Control Center server administration on page 249

Chapter 33: Networking Service Monitor configuration

Configure Contact Center Manager Server Service Monitor to monitor the services status on various servers.

Prerequisites to Networking Service Monitor configuration

- Install all Contact Center Manager Server nodes. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Install all Contact Center Manager Administration servers. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Commission all Contact Center Manager Servers. See *Avaya Aura® Contact Center Commissioning* (NN44400-312).
- Commission all Contact Center Manager Server Administration servers. See *Avaya Aura® Contact Center Commissioning* (NN44400-312).
- Install the Network Control Center server software. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Install the Contact Center License Manager software. See *Avaya Aura® Contact Center Installation* (NN44400-311).

Navigation

- Changing the site to monitor on page 246
- Closing the Networking Service Monitor on page 246
- Refreshing the service status on page 247
- Setting the default site information (client machine) on page 247
- Adding a site on page 247

Changing the site to monitor

About this task

Change the site to monitor one or more sites in the Contact Center Manager Server network.

Procedure

1. Log on to the NCC server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **System Monitor**.
3. On the left panel, double-click **Other Sites** to display the sites on the network.
4. To monitor a site in the list, double-click the site name.

Closing the Networking Service Monitor

About this task

Close the Network Service Monitor when you no longer need the application to monitor network services.

Procedure

1. Right-click the Contact Center Manager Server Service Monitor icon in the system tray.
2. From the resulting menu, click **Exit Contact Center Manager Service Monitor**.

   You can not exit the application by clicking an exit button. Running the application again restores the existing instance of the Contact Center Manager Server Service Monitor.

Refreshing the service status

About this task

Contact Center Manager Server Service Monitor has an internal timer to refresh the status of the service from time to time. Manually refresh the service status to display the current status.

Procedure

Double-click a service in the list to refresh its status.

OR

Click **Refresh All** to refresh the status of all services.

Setting the default site information (client machine)

About this task

A client user can change the default site information at any time. Changes take effect at the next startup of the Contact Center Manager Server Service Monitor.

Procedure

1. Click **Set Site**.
2. Enter the new IP address.

Adding a site

Before you begin

- Log on to the Network Control Center as Administrator.
- Start the Contact Center Manager Server Configuration utility in administrator mode.

About this task

Add a site using the Contact Center Manager Server Configuration utility on the Network Control Center with administration access.

Procedure

1. In the **Nbconfig** utility dialog box, click the **Site Table** tab.
2. Click **Add**.
3. Enter the contact center subnet IP address of the site to add.
4. Click **OK**.

Chapter 34: 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

- Install all Contact Center Manager Server nodes. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Install all Contact Center Manager Administration servers. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Install the Network Control Center server software. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Install the Contact Center License Manager software. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Commission each Contact Center Manager Server in your contact center. See *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Adding a site to the NCC on page 250
- Deleting a site from the NCC on page 251
- Adding access classes on page 252
- Adding a site in Contact Center Manager Administration on page 253

- Configuring Landing Pads for Universal Networking on page 254
- Configuring network communication parameters on page 255
- Synchronizing site information on page 257
- Adding a network skillset on page 258
- Deleting a network skillset on page 259
- Configuring network skillset properties on page 260
- Configuring Agent Order Preference on page 261
- Configuring the routing tables on page 261
- Configuring routing table assignments on page 262
- Configuring the historical statistics collection on page 264
- Configuring MCDN network CDNs on page 265
- Configuring DNIS Network CDNs on page 266

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. Click **Start** > **Run**.
2. In the **Run** text box, type `nbconfig -admin`.
3. In the **Nbconfig** dialog box, click the **Site Table** tab.
4. Click **Add**.
5. In the **Add Site** dialog box, in the **CLAN IP Address** box, type the CLAN IP address of the server.
6. Click **OK**.
   The server is added to the list in the site table.

7. Repeat step 3 on page 250 to step 5 on page 250 for each server in your network.
8. Click **Verify**.
   This verifies the connection to the nodal servers.
9. 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.
10. 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.
11. Click the **Address Table** tab.
    The communication addresses of the new servers appear on the Address Table page.

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, 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 254.
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 254.
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 Configuration – Avaya CS 1000 Integration* (NN44400-512).

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. Select the **Acquired?** check box for the CDN (Route Point) Landing Pad.
10. Click any other row of the table to acquire the CDN (Route Point) Landing Pad.
11. To configure a **DNISs** Landing Pad, in the left pane, click the **DNISs** folder.
12. Select the **Landing Pads** tab.
13. In the **Name** box, type a name for the DNIS Landing Pad.
14. In the **Number** box, type the number for the DNIS Landing Pad. This number must match the DNIS number configured on the PABX.
15. 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.
16. In the **Description** box, type an optional description for the DNIS Landing Pad.
17. 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 262 to step 9 on page 262 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 263 to step 9 on page 263 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 264.

    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 *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (NN44400-510).

- 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 Configuration – Avaya CS 1000 Integration* (NN44400-512).

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 Configuration – Avaya CS 1000 Integration* (NN44400-512).

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 Configuration – Avaya CS 1000 Integration* (NN44400-512).
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 VI: Communication Control Toolkit Server

- Communication Control Toolkit server fundamentals on page 271
- Communication Control Toolkit server configuration on page 275
- Resource bulk management on page 279

Chapter 35: Communication Control Toolkit server fundamentals

Communication Control Toolkit is a client/server application that helps you implement Computer-Telephony Integration (CTI) for installed and browser-based client integrations. For PBX, the Communication Control Toolkit facilitates the integration of Contact Center, Knowledge Worker, and Self Service solutions with your client applications. This chapter provides some background information for the Communication Control Toolkit server and the applications.

Navigation

- Automatic Call Distribution on page 271
- Communication Control Toolkit Administration Console on page 272
- Communication Control Toolkit Web Administration on page 272
- Trace Control Utility on page 272
- Programming interfaces on page 272
- Communication Control Toolkit Reference Client on page 274

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 on the Communication Control Toolkit server 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 Manager Administration – Client Administration* (NN44400-611).

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 your CCT server, 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 Knowledge Worker, 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 . Two abstraction layers are also available:

- the lite Communication Control Toolkit API
- the graphical Communication Control Toolkit API

You can implement these layers using the full Communication Control Toolkit API . They provide 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.

One example of a CCT client application is the Agent Desktop. If your contact center is licensed to handle only telephony calls, you can install the Agent Desktop telephony toolbar on the Communication Control Toolkit server to provide agents with a soft phone on their desktop. The Avaya Aura® Agent Desktop telephony toolbar is a component on the Contact Center Multimedia server software.

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 full 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 36: Communication Control Toolkit server configuration

This section outlines the procedures necessary to configure the Communication Control Toolkit (CCT) server.

You use the Communication Control Toolkit Console application on the CCT server to configure licensing and deployment type.

Navigation

- Configuring CCT licensing on page 275
- Configuring CCT deployment type on page 277

Configuring CCT licensing

Before you begin

- Contact Center License Manager is installed.
- Communication Control Toolkit is not co-resident with Contact Center Manager Server.

About this task

Configure CCT licensing with the IP address of the server where Contact Center License Manager is installed and configured.

CCT consumes licenses as required. For example, every time a CCT client logs in as a CCT user and opens a terminal, CCT automatically uses a license. When a terminal is released the license is released.

CCT License Configuration is disabled when CCT is installed co-resident with CCMS. Use the CCMS Server Configuration tool to configure licensing on a co-resident server.

Procedure

1. Log on to the Communication Control Toolkit server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.

3. Expand **Communication Control Toolkit**.
4. Expand **Server Configuration.**
5. Click **License Configuration.**
6. In **License Configuration** pane, on the right hand side, under **Primary License Manager Server**, in the **IP Address** box, type the IP address for the server on which the License Manager is installed.
7. Under **Secondary License Manager Server**, in the **IP Address** box, type the IP Address for the server on which the secondary License Manager is installed.

   Important:

   The Secondary License Manager Server IP Address section is available only if corporate licenses are installed.
8. From the **License Type** list, select Nodal or Corporate.
9. In the Actions pane on the right, select **Apply changes**.

Variable definitions

Name	Description
License Type	The type of license for the License Manager. Nodal—The license applies to only one installation of CCMS. You cannot configure the Secondary License Manager for a Nodal license. Corporate—The license applies to a collection of Contact Center Manager Servers. Secondary License Manager is available only for Corporate licenses.
Primary License Manager Server IP Address	The IP address of the server on which the License Manager application is installed. CCT License Configuration is disabled when CCT is installed co-resident with CCMS.
Secondary License Manager Server IP Address	The optional IP address of the server on which the backup License Manager application is installed. CCT License Configuration is disabled when CCT is installed co-resident with CCMS.

Configuring CCT deployment type

Before you begin

- Understand the network requirements for your installation of CCT (co-resident, stand-alone, or multimedia).
- Know how to restart the CCMS and CCT services.

About this task

Configure the deployment type for the CCT server to manage the contact routing for your network configuration. The Deployment Type dialog is used on a standalone CCT server to specify whether or not the Communication Control Toolkit server integrates with a Contact Center Manager Server to provide Contact Center functionality.

The CCT deployment type dialog box is disabled when CCT is installed co-resident with CCMS.

Procedure

1. Log on to the Communication Control Toolkit server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
3. Expand **Communication Control Toolkit**.
4. Expand **Server Configuration**.
5. Select **Deployment Type**.
6. In the **Deployment Type** dialog box, select the deployment type for your Communication Control Toolkit.
7. In the **CCMS Server Hostname** box, type the name of the Contact Center Manager Server.
8. In the **Actions** pane on the right, select **Apply changes**.
9. Stop and restart the Communication Control Toolkit services.

Variable definitions

Name	Description
Communication Control Toolkit Deployment Type	Choose the deployment type for Communication Control Toolkit based on your network configuration. This option is always disabled if CCT is co-resident with CCMS. CCT Installation (Contact Center only) if your Contact Center is licensed for multimedia contacts and the CCT server software is installed on the same server as CCMS. Choose Stand-alone CCT installation (Contact Center only) if your Contact Center is licensed for multimedia contacts and the CCT server software is not installed on the same server as CCMS. Choose CCT installation (Contact Center only) co-resident with CCMS where CCMM is not part of the solution and OpenQ feature is disabled on the CCMS server OR Standalone CCT installation (Contact Center or Knowledge Worker) where CCMM is not part of the solution and the OpenQ feature is disabled on the CCMS server.

Chapter 37: 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

- Understand the licensed features for your contact center. Specific resource or resource types may be excluded from your license package.

Navigation

- Importing Windows users on page 280
- Importing Avaya Communication Server 1000 data on page 281
- Importing workstations from the domain on page 284
- Importing bulk resources on page 285
- Exporting bulk resources on page 286

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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **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**, a **Login Name**, or a **First Name**, a **Last Name**.
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. 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

- Connect a COM cable from a server (not the Communication Control Toolkit server) or workstation to the PABX.
- Install Hyperterminal using a serial connection.
- 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 the 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 the user to carry out testing of the data import facility without modifying the database contents or enables them 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, create a switch configuration text file to capture the Avaya Communication Server 1000 data required to configure Communication Control Toolkit.

Do not use the Communication Control Toolkit server to import the information directly from the switch; Hyperterminal, when installed, interferes with the Telephony services and they remain running.

Procedure

1. Open a text editor on the server where the Hyperterminal is installed.
2. Create a new text file called **download.txt**.
3. Click **Start** > **All Programs** > **Accessories** > **Communications** > **HyperTerminal** to connect to the Avaya Communication Server 1000.
4. Type a name for the connection.
5. Click **OK**.
6. On the **Connect To** dialog box, in the **Connect using** list, select COM1 or the COM port connected to the Avaya Communication Server 1000 switch.
7. Click **OK**.
8. In the **COM properties** dialog box, verify the data is correct or make necessary changes.
9. Click **OK**.
10. From the **Transfer** menu, select **Capture Text**.
11. In the **Capture Text** dialog box, type the location and name of the text capture file in the **File** box, for example, type the location and name of the **download.txt** file created in step 2 on page 282.
12. Click **OK**.
13. At the prompt, type `logi admin1` to log on to the switch.

14. Type your user ID and your password for the switch.
15. If the prompt is not present, continue to press `Enter` until the prompt appears.
16. Browse to the download.txt file, and then click **Start**.
17. 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.

18. To return to the prompt, enter `****` (Shift + 8888).
19. Press `Enter`.
20. 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.

21. Type `logo`.
22. Press `Enter`.
23. Copy the **download.txt** file to the Communication Control Toolkit server.
24. Log on to the Communication Control Toolkit server.
25. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
26. Expand **Communication Control Toolkit**.
27. Expand **Bulk Provisioning**.
28. Select **Import CS 1000 Data**.
29. Select **Passive** for the Avaya Communication Server 1000 Provider.
30. Select **Input File**. This opens a file explorer to select the Avaya Communication Server 1000 data capture file you copied in step 23 on page 283.
31. 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.
32. To import the data into the database select **Automatically import data after conversion.**

33. 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
34. 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 are 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.

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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **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 name contains the specified string (case insensitive) are returned.
Name begins with	Workstations whose name begin with the specified string (case insensitive) are returned.
Name ends with	Workstations whose name ends 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. On the Communication Control Toolkit server, click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
2. In the CCT Console window, expand **Communication Control Toolkit**.
3. Expand **Bulk Provisioning Tools**.
4. Click **Data Import/Export Tools**.
5. In the **Format** drop-down box, select **Standard XML** or **Flattened XML**.
6. In the **Actions** pane select **Import**, a file explorer window is displayed.
7. 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.
8. 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. On the Communication Control Toolkit server, click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
2. In the CCT Console window, expand **Communication Control Toolkit**.
3. Expand **Bulk Provisioning Tools**.
4. Click **Data Import/Export Tools**.
5. In **Setup**, select **Standard XML** or **Flattened XML** in the Format drop down box.
6. In **Setup**, select the **resources** to export.
7. In the **Actions** pane select **Export**, a file explorer window is opened.
8. 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, and agent 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, and agent groups. You can choose all resources or individual resources by selecting the appropriate check boxes under Resources.
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

Name	Description
	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 VII: ContactCenterMultimedia

- Contact Center Multimedia fundamentals on page 291
- General configuration on page 305
- Outbound configuration on page 321
- E-mail configuration on page 323
- Voice mail configuration on page 365
- Scanned document configuration on page 377
- Fax configuration on page 389
- Instant message configuration on page 401
- Short Message Service configuration on page 413
- Web communications configuration on page 425
- Predictive Outbound administration on page 447
- Agent Desktop configuration on page 453
- User configuration on page 471
- Data collection and management on page 475

Chapter 38: Contact Center Multimedia fundamentals

Use the Contact Center Multimedia server 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 Release 6.2 include the following:

- voice contacts
- e-mail messages
- Short Message Service (SMS) text messages
- faxed documents
- scanned documents
- voice mail messages
- outbound contacts
- Web communications contacts
- instant messages (for SIP-based PABXs)

The Voice Contact Center Manager Server and Communication Control Toolkit handle and route 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.

Navigation

- E-mail contact type on page 292
- SMS text messages, faxes, scanned documents, and voice mail attachments on page 297
- Outbound contact type on page 299
- Web communications on page 302

- Instant Messaging on page 302
- Office hours on page 303

E-mail contact type

Use e-mail messages to communicate with clients by using an e-mail provider such as Microsoft exchange. The following figure shows the life cycle of an e-mail contact from the time it is received by the e-mail server until it is routed to an agent.

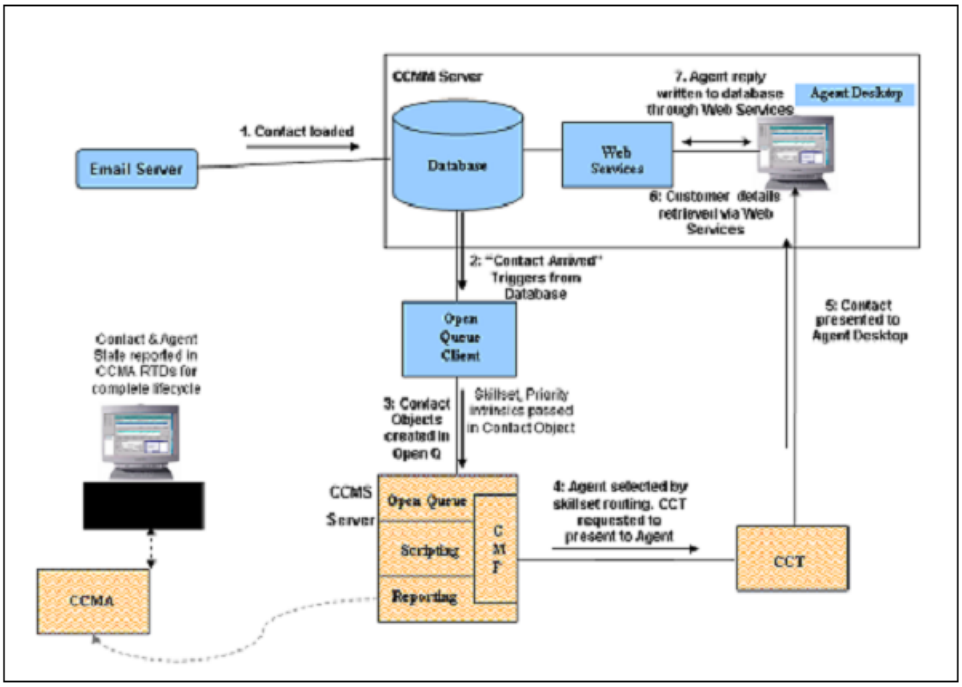


Figure 4: E-mail contact life cycle

You can route e-mail 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 contact is received, the text is in the e-mail message, or who sent it. The e-mail message is assigned to a skillset with a priority and then to an agent who can handle the contact based on the received criteria.

The e-mail contact type has several components:

- E-mail rule groups on page 293
- Recipient mailboxes on page 293
- Inbound e-mail settings on page 294

You must configure e-mail settings for e-mail messages leaving your contact center as a campaign or in response to customer e-mail messages.

- Outbound e-mail settings on page 294
- Character encoding for outgoing e-mail messages on page 294

You can configure the e-mail message contact type for international languages, see Asian e-mail on page 295.

You can view real-time traffic reports for your e-mail messages. Configure the date and time for which you want to review the e-mail traffic in your contact center. See E-mail traffic reports on page 295.

All agent handling of e-mail messages occurs in the Avaya Aura® Agent Desktop. Contact Center Manager Administration manages other real-time and historical reporting. See Agent Desktop on page 296, Contact Center Manager Administration on page 296, and Web services on page 297.

E-mail rule groups

Rules determine how a multimedia contact is routed based on information about the e-mail 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 e-mail or by looking at who sent the message.

Rule groups are collections of rules that evaluate the incoming e-mail 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 and e-mail contact to a specific skillset with a priority. The procedure for configuring the default rule is in *Avaya Aura® Contact Center Commissioning* (NN44400-312).

For example, a magazine advertises an investment strategy. Customers can learn more about the investment by sending an e-mail with “Good Investing” in the subject line to a specific address. Create a rule to search incoming e-mail messages for “Good Investing.” If the e-mail 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 e-mail message is received.

Recipient mailboxes

Contact Center Multimedia polls specific recipient mailboxes on the e-mail server based on a list of mailboxes defined in the Multimedia Administrator recipients list. The e-mail retrieved

from these mailboxes is routed based on defined rules applied to either a mail store or an alias. You must ensure that enabled e-mail addresses configured in your Email Manager are already configured on your corporate e-mail server.

The recipient mailbox has a default rule group assigned to handle the e-mail 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, and faxes and scanned documents attach a .tiff file to an e-mail message handled by the Email Manager. An SMS text message also uses the Email Manager to route text messages.

Inbound e-mail settings

Perform this optional configuration if you are licensed for e-mail contacts.

You can configure the following optional e-mail settings:

- how frequently you scan the e-mail server for new messages
- the location in which to store attachments
- the text searched when you use keywords for rules

Outbound e-mail settings

Configure outgoing e-mail mailbox settings to identify who responds to the e-mail message from the customer. For outgoing e-mail, you can change the character encoding of the message to display the e-mail message with the correct characters.

The response can contain the e-mail address to which the customer sent the original e-mail message or a general corporate e-mail address configured for each skillset. Agent-initiated messages are always sent from an e-mail address associated with a skillset.

E-mail messages must be relayed through the e-mail server, not forwarded to another party if you manage e-mail messages on behalf of an external source. Sending e-mail messages preserves the original To address that is used for e-mail rule administration and outgoing e-mail addresses.

Character encoding for outgoing e-mail messages

The Contact Center Multimedia Email Manager replies to an e-mail message using the same characters as the inbound e-mail. For example, if an e-mail 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 e-mail client can understand the format of the message sent from the contact center.

If the customer sends an e-mail message in English and receives either an agent response or an automatic response in another character set, you cannot tell if the customer e-mail 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 e-mail.

If the original e-mail is encoded with the Latin-1 characterset (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 e-mail can be perceived as a blank e-mail. Avaya recommends that only contact centers in Europe use Latin-9 encoding.

Asian e-mail

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 Web site as a legitimate Web site.

Phishing e-mail messages contain links to malicious Web sites that look similar to legitimate business Web sites. 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 e-mail 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 interpret the native characters.

Contact Center Multimedia supports IDNs. You or a customer can enter a punycode e-mail address. The receiving client can render the native characters.

E-mail traffic reports

Reports appear in the CCMM Administration utility to show the current status of the e-mail 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 e-mail 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 e-mail 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.

AgentDesktopEmail

Agents use Agent Desktop to process e-mail contacts. When an e-mail message arrives at the contact center, contacts are routed to Agent Desktop, and agents can perform the following activities:

- Accept or reject an e-mail message.
- Review and update customer information.
- Create a reply.
- Select a prepared response to send to the customer contact.
- Select a activity code to record the result of the customer contact.

For more information about Agent Desktop, see the *Avaya Aura® Agent Desktop User Guide* (NN44400-114).

ContactCenterManagerAdministrationE-MailContactType

Use Real-Time Reporting and Historical Reporting in Contact Center Manager Administration to create and run real-time and historical reports for e-mail contacts.

For more information about the reporting and performance statistics, see the following documents:

- *Avaya Aura® Contact Center Performance Management Data Dictionary* (NN44400-117)
- *Avaya Aura® Contact Center Performance Management* (NN44400-710)
- *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611)

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 e-mail contacts received into monitored mailboxes.

The Web services provide the following functions for external applications:

- agent authentication with CCMM Database
- ability to read e-mail contacts
- ability to reply to and forward e-mail contacts

For more details, see the SDK documentation.

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 e-mail address.

A fax (short for facsimile) is a document sent over a phone line. Faxes are forwarded by a fax server to an e-mail 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 e-mail 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 e-mail 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 298.

You can view traffic report summaries for each type of contact. See Traffic reports on page 298.

Use the Agent Desktop to open and reply to SMS, faxes, scanned documents, and voice mail contacts. See Agent Desktop on page 299.

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.

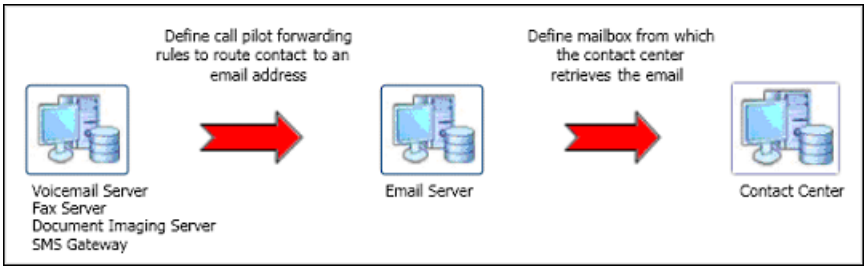


Figure 5: Contacts attached to e-mail cycle

Mailbox configuration

You can configure the following properties for the contacts:

- POP3 Server (for receiving e-mail 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 e-mail 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.

AgentDesktopEmailSkillset

Agents use Agent Desktop to process e-mail contacts. When an e-mail message arrives at the contact center, contacts are routed to a skillset, and agents can perform the following activities:

- Accept or reject an e-mail message.
- Review and update customer information.
- Create a reply.
- Select a prepared response to send to the customer contact.
- Select a activity code to record the result of the customer contact.

For more information about Agent Desktop, see the *Avaya Aura® Agent Desktop User Guide* (NN44400-114).

Outbound contact type

The outbound contact type is an outgoing call made by agents to customers for sales or marketing.

The following figure shows how outbound contacts interact with Contact Center Manager Administration, Contact Center Multimedia, and Contact Center Manager Server.

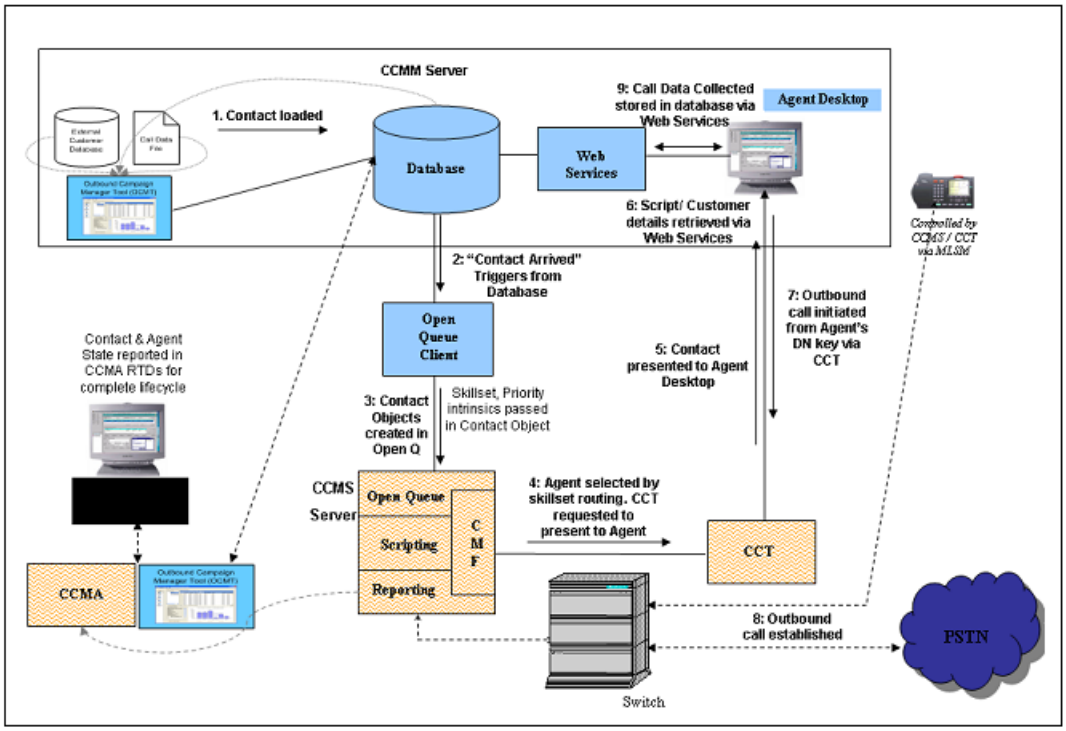


Figure 6: Outbound contact type routing

Contact Center Outbound consists of several components:

- Outbound Campaign Management Tool on page 300
- Campaign Scheduler on page 301
- Agent Desktop on page 301
- Contact Center Manager Administration on page 301
- Web services on page 302

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.

Contacts are queued to Contact Center Manager Server at the configured rate. By default, the Campaign Scheduler presents outbound contacts every 60 seconds.

AgentDesktopOutboundContacts

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.

For more information about Agent Desktop, see the *Avaya Aura® Agent Desktop User Guide* (NN44400-114).

ContactCenterManagerAdministrationOutboundContactType

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

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

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
- agents can handle multiple contacts

Office hours

For all delayed time contacts, including e-mail 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.

Chapter 39: 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

- Log on to the Contact Center Manager Administration application. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Configuring the system license on page 306
- Configuring the reporting credentials on page 306
- Adding administrators on page 307
- Removing administrators on page 308
- Configuring office hours on page 308
- Configuring holidays on page 309
- Applying office hours on page 310
- Viewing real-time traffic reports by contact on page 311
- Configuring the displayed date for traffic reports on page 311
- Configuring Web On Hold comfort groups for a Web communications skillset on page 312
- Removing a Web On Hold comfort group for a Web communications skillset on page 313
- Configuring Web communications comfort groups for a Web communications skillset on page 314
- Removing a Web communications comfort group from a Web communications skillset on page 314
- Configuring a Geographic Alternate Communication Control Toolkit server on page 315
- Deleting a Geographic Alternate Communication Control Toolkit server on page 316

- Configuring an LDAP server on page 316
- Configuring a Phonebook LDAP server on page 318
- Configuring a Predictive server on page 319

Configuring the system license

Before you begin

- Log on to the Contact Center Manager Administration application.

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.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **General Administration**.
3. Click **General Settings**.
4. Under **License Type**, select the type of license used in your contact center.
5. Click **Save**.

Configuring the reporting credentials

Before you begin

- Log on to the Contact Center Manager Administration application.

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.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **General Administration**.
3. Click **General Settings**.
4. 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.

   OR

   Type the new password in the **New Password** and **Confirm Password** boxes.
6. Click **Save**.

Adding administrators

Before you begin

- Log on to the Contact Center Manager Administration application.

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 the predictive support tool or some Web services.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 e-mail address.
7. In the **Password** section type and confirm your password.
8. Click **Save**.

Removing administrators

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Remove an administrator account that you no longer require in your contact center.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **General Administration**.
3. Click **Administrator Settings**.
4. Select the administrator account to remove.
5. Click **Delete**.

Configuring office hours

Before you begin

- Know the office hours of the contact center.
- Log on to the Contact Center Manager Administration application.

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 service levels for contacts that may have a delayed response such as e-mail, 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 e-mail rules to determine the skillset to which to route the contact. The e-mail 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.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 309 and step 7 on page 309 for every day of the week.
9. Click **Save**.

Configuring holidays

Before you begin

- Identify the closed days of the contact center.
- Log on to the Contact Center Manager Administration application.

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 may have a delayed response such as e-mail, 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 e-mail rules to determine the skillset to which to route the contact.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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

- Log on to the Contact Center Manager Administration application.
- Create a calendar template with office hours or holidays. See Configuring office hours on page 308 or Configuring holidays on page 309.

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 e-mail settings for the contact center.

You can respond to e-mail messages by selecting the office hours calendar to send automatic messages to incoming e-mail contacts. You can select which rule group to apply the global office hours to. For more information, see Creating or changing rules on page 347.

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 e-mail on page 328.

Procedure

1. In the Contact Center Multimedia Administration application, click **E-mail**.
2. In the left column, click **General Settings**.
3. Under **Office Hours**, select the **Out of hours treatment is enabled** check box to automatically send an out-of-office type message to the customer when the contact center is closed.
4. Select the calendar you want to use to determine the business hours for your contact center.
5. Select the automatic response for the out of office hours notice.
6. Click **Save**.

Viewing real-time traffic reports by contact

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

For e-mail, 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 311.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. Select a media type that supports the traffic report views (**SMS**, **E-mail**, **Fax**, **Scanned Documents**, and **Voice Mail**).
3. Click **View Reports**.

Configuring the displayed date for traffic reports

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

For e-mail, 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.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. Select a media type that supports the traffic report views (**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

- Log on to the Contact Center Manager Administration application.
- 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 439.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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

- Log on to the Contact Center Manager Administration application.
- 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.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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

- Log on to the Contact Center Manager Administration application.
- 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 442.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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

- Log on to the Contact Center Manager Administration application.
- 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.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 Alternate Communication Control Toolkit server

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **General Administration**.
3. Click **Server Settings**.
4. Click **New**.
5. In the **Server Type** list, select the **Geographic Alternate CCT Server** option.
6. In the **Hostname** box, type the name of the CCT server.
7. Click **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

- Log on to the Contact Center Manager Administration application.
- 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **General Administration**.
3. Select the **Geographic Alternate CCT Server** to delete.
4. Click **Delete**.
   The warning dialog box appears.
5. Click **OK** to confirm the decision.
6. Click **Close**.

Configuring an LDAP server

Before you begin

- Log on to the Contact Center Manager Administration application.

Important:

The LDAP directory server requires authentication to enable searching. Enter the user credentials of a network domain administrator in these boxes. The user name can take

the format DOMAIN\username (for example, EUROPE\adminuser) or username@DOMAIN (for example, adminuser@europe.com).

About this task

The Lightweight Directory Access Protocol (LDAP) server contains databases of customer addresses and other information to use when handling e-mail contacts in the Agent Desktop. Agents can select recipients from the LDAP list when composing an e-mail message.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **General Administration**.
3. Click **Server Settings**.
4. Select the **Directory LDAP Server**.
5. Click **Edit**.
6. Click **Enable Address Book Retrieval** to enable the directory.
7. Type the **Username** and **Password** for the administrator on the LDAP server.
8. In the **Search Base** field, specify the preciseness of the LDAP search. For example, in a large enterprise of tens of thousand of people, it may not be 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.
9. In the **Polling Interval** box, type the polling interval, in hours, for the interval between polls for the e-mail server lookup.
10. In the **Server Name** box, type the server name for the e-mail server that you use to get e-mail addresses.
11. Click **Edit Server** to change the properties of the e-mail server. The default port number for the LDAP server is 389.
12. Click **Test** to test the connection to the LDAP server.
13. Click **Save**.

Configuring a Phonebook LDAP server

Before you begin

- Log on to the Contact Center Manager Administration application.
- Ensure that the LDAP server that you use for voice contacts is commissioned and operational.
- Ensure that the Contact Center LDAP Phone Book check box present in the Multimedia, Agent Desktop Configuration, Advanced Settings page is enabled.

Important:

To retrieve contacts from the LDAP server, ensure that the **Enable Address Book Retrieval** check box is selected. See Configuring an LDAP server on page 316.

About this task

Configuring a Phonebook LDAP server provides agents with a list of contacts during a voice call.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **General Administration**.
3. Click **Server Settings**.
4. Click **New**.
5. In the **Server Type** list, select the **Phonebook LDAP Server** option.
6. Click **Edit Server**.
7. In the **Server Name** box, type the server name.
8. In the **Server Port** box, type the port number for the server.
9. Click **Save**.
10. Click **Test** to test the username, password, and search base, by connecting to the configured server to retrieve contacts.
11. Click **Save**.

Configuring a Predictive server

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Configuring the Predictive server includes configuring the following:

- The SER solutions server that imports the customer dialing numbers and dials the numbers to the customers at the prescribed rate.
- The Predictive Outbound solutions application server on which the administration software resides, or the CPSE2 server.
- The SER solutions server that contains the statistics for reporting predictive outbound data, or Portfolio server.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **General Administration**.
3. Click **Server Setting**.
4. Click **New**.
5. In the **Server Type** list, select the **TSP Dialer** option.
6. In the **Server Name** box, type the server name.
7. In the **Server Port** box, type the port number for the server.
8. Click **Save**.

Chapter 40: 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 Manager Administration – Client Administration* (NN44400-611).

Prerequisites for Outbound configuration

- Ensure that you are licensed for Outbound contacts in your contact center.
- Ensure that the route points (CDN) are configured in Contact Center Manager Administration.
- Log on to the Contact Center Manager Administration application. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Configuring a route point for an Outbound skillset on page 321

Configuring a route point for an Outbound skillset

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 41: E-mail configuration

Use this chapter to set up your contact center with the optional configurations for routing e-mail contacts to fulfill your customer requirements.

When you commission your contact center, you configure the e-mail server, a default e-mail skillset, and a default recipient with at least one rule group. The default settings ensure e-mail messages go only to an agent with the ability to handle e-mail messages. You can customize your contact center with additional skillsets, rule groups and e-mail 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 e-mail contact is assigned to based on the input for routing contacts. Use automatic suggestions for the agent to reply quickly to an e-mail 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 e-mail settings, such as which skillset to use as a reply address and a list of e-mail 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 e-mail messages that are routed using the inbound and outbound e-mail options.

Reports appear in the Contact Center Multimedia Administration utility to show the current status of the e-mail traffic. The following reports appear when you select E-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.

- 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.
- 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 e-mail contact spends in queue while the contact center is open.

You can configure general e-mail settings to minimize space and format special characters for other languages.

Prerequisites for e-mail configuration

- Ensure that you are licensed for e-mail contacts.
- Log on to the Contact Center Manager Administration application. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

Reviewing required e-mail contact configuration

- Configuring the e-mail server names on page 325
- Adding an e-mail server on page 326
- Deleting an e-mail server on page 327
- Configuring skillsets for e-mail on page 328
- Creating or changing a recipient mailbox on page 329
- Creating or changing an alias for a recipient mailbox on page 331
- Deleting a recipient mailbox on page 333

E-mail routing configuration

- Updating the system default rule on page 334
- Updating the system delivery failure rule on page 336
- Creating or changing a keyword group on page 337
- Deleting a keyword from a keyword group on page 339
- Deleting a keyword group on page 340
- Creating or changing prepared responses on page 340
- Deleting prepared responses on page 343
- Removing attachments from prepared responses on page 344
- Promoting suggested responses on page 344
- Creating or changing a sender group on page 345
- Deleting a sender group on page 346
- Deleting a sender from a sender group on page 347
- Creating or changing rules on page 347
- Enabling a rule on page 350

- Disabling a rule on page 351
- Deleting a rule on page 351
- Creating or changing rule groups on page 352

Outgoing e-mail configuration

- Configuring the e-mail settings on page 353
- Changing the character encoding for outgoing e-mail on page 355
- Selecting the outgoing e-mail address on page 356
- Barring e-mail addresses on page 357
- Deleting a barred e-mail address on page 357

Other e-mail configuration

- Configuring Microsoft Exchange 2007 for sending outgoing e-mail on page 358
- Enabling SSL on the Email Manager on page 359
- Enabling SMTP Authentication on your e-mail server on page 361
- Determining if SMTP Authentication is enabled on page 362

Configuring the e-mail server names

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Configure the e-mail server names to identify the inbound server (POP3) for e-mail messages received by the contact center and the outbound server (SMTP) for e-mail messages sent by the contact center.

If you configured the e-mail servers during installation and the names of the inbound and outbound e-mail servers remain unchanged, you can skip this procedure.

You can configure secondary inbound and outbound e-mail servers. If a primary e-mail server fails, the e-mail retrieved during the failure is duplicated in the Multimedia database when you restore the primary server.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **General Administration**.
3. Click **Server Settings**.
4. Under **Edit Current Servers**, select **Inbound POP3 Server**.

5. Click **Edit**.
6. In the **Primary Hostname** box, type the name of the server that receives or sends e-mail messages.
7. In the **Port Number** box, type the port number for the e-mail server.
8. If you have a backup e-mail server, in the **Secondary Hostname** box, provide a host name for the backup server.
9. Click **Save**.
10. Under **Edit Current Servers**, select **Outbound SMTP Server**.
11. Click **Edit**.
12. In the **Primary Hostname** box, type the name of the server that receives or sends e-mail messages.
13. In the **Port Number** box, type the port number for the e-mail server.
14. If you have a backup e-mail server, in the **Secondary Hostname** box, provide a host name for the backup server.
15. In the **Advanced SMTP Authentication** box, select the SMTP authentication, if required, for your outbound e-mail server.
16. Click **Save**.

Variable definitions

Name	Description
Port Number	Port number for the e-mail server.
Primary Hostname	The name of the server that receives e-mail messages.
Secondary Hostname	Name of a secondary e-mail server, if one is available in your contact center.

Adding an e-mail server

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Add or update the e-mail server for your Contact Center Multimedia server so you can poll multiple e-mail servers in your contact center for e-mail messages to be routed. You can

retrieve e-mail messages for the contact center only if you are licensed to use the e-mail feature.

Important:

Contact Center Multimedia supports only adding a maximum of 5 POP3 servers and 5 SMTP servers.

Procedure

1. In the Contact Center Manager Administration, click **Multimedia**.
2. In the left column, click **General Administration**.
3. Click **Server Settings**.
4. Click **New**.
5. In the **Server Type** box, choose either **Inbound POP3 Server** or **Outbound SMTP Server** as your server type.
6. In the **Primary Hostname** box, type the host name of the e-mail server to add.
7. In the **Port Number** box, type the port number for the e-mail server to add.
8. In the **Secondary Hostname** box, type the host name for your alternative secondary e-mail server.
9. In the **Advanced SMTP Authentication** box, select the SMTP authentication, if required, for your outbound e-mail server.
10. Click **Save**.

Deleting an e-mail server

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Delete an e-mail server or other nonessential server if the server is no longer required.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. On the left side, click **General Administration**.
3. Click **Server Settings**.
4. Select the sever to delete.
5. Click **Delete**.

6. Click **OK** to confirm the deletion.
7. Click **Close**.

Configuring skillsets for e-mail

Before you begin

- Log on to the Contact Center Manager Administration application.
- If desired, configure an office hour template. See Configuring office hours on page 308 and Configuring holidays on page 309.

About this task

Configure a route point for each skillset, and 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 Web site by adding the URL and other promotional information or disclaimer text to every message.

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 e-mail settings to this skillset.

Procedure

1. In the Contact Center Manager Administration, click **Multimedia**.
2. In the left column, 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. If applicable, in the **Chat History Header** box, select the header to appear in the chat text.

10. Click **Save**.

Creating or changing a recipient mailbox

Before you begin

- Ensure that any enabled e-mail address you want to configure in the Email Manager is already configured on your corporate e-mail server.
- Log on to the Contact Center Manager Administration application.

About this task

Create a recipient e-mail box to ensure that at least one e-mail 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 e-mail server and handle contacts based on the recipient address.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **E-mail**.
3. Click **Recipient Addresses**.
4. Click **New**.

   OR

   Select a recipient address, and click **Edit**.
5. From the **Mailbox Type** list, select **Mail Store**.
6. Under **Mailbox Details**, in the **Mailbox** box, type the SMTP mailbox name.
7. In the **Domain** box, type the domain for your e-mail server.
8. In the **Display Name** box, type the name to appear in the e-mail From address.
9. In the **Password** box, type the password for the mailbox.

   Important:

   When you change a password on the e-mail server, you must update this password in the Multimedia Administrator.
10. In the **Confirm Password** box, type the same password you typed in the Password box.
11. In the **Inbound POP3 Server** box, ensure that the host name of your POP3 server appears.

12. In the **Inbound Mail Threshold** box, type the maximum number of e-mail 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** box, ensure that the host name of your SMTP server appears.
14. In the **Rule Group** box, 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 e-mail From address. For example, Sales Department.
Domain	The domain name for the e-mail server.
Mailbox	The name of a mailbox on the e-mail server. If the Contact Center Multimedia server is in the same domain as the e-mail 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 e-mail 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 e-mail 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.
Password and Confirm	The password used to access the mailbox on the e-mail server. Type the password in the Confirm box to ensure accuracy.

Name	Description
Inbound Mail Threshold	The maximum number of e-mail 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.
Inbound (POP3) Server	The name of the e-mail server that handles e-mail messages coming into the contact center.
Outbound (SMTP) Server	The name of the e-mail server that delivers e-mail messages that leave the contact center.

Creating or changing an alias for a recipient mailbox

Before you begin

- Ensure that any enabled e-mail address you want to configure in the Email Manager is already configured on your corporate e-mail server.
- Configure a mail store recipient mailbox. See Creating or changing a recipient mailbox on page 329.
- Log on to the Contact Center Manager Administration application.

About this task

Create an alias, or another name, for the recipient e-mail box.

For example, the mailbox general@magscripts.com can have the aliases carz@magsubscriptions.com and planez@magsubscriptions.com. E-mail messages addressed to either alias are forwarded to the general@magscripts.com mailbox. The Email Manager routes the e-mail messages according to the alias-based rules.

Aliases can be useful to filter e-mail messages. For example, you can define an alias for a short promotional period after which e-mail messages that arrive at that alias are discarded.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 e-mail server.
8. In the **Display Name** box, type the name of the alias set up on the e-mail 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** box if you configure an inbox as an alias. If SMTP authentication is enabled on your e-mail server, and you use aliases, log on to the SMTP server with a different user name.
12. 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 e-mail server, you must update this password in the Multimedia Administrator.
13. In the **Confirm Password** box, type the same password you typed in the Password box.
14. Click **Save**.

Variable definitions

Name	Description
Alias	An alias is an address that forwards all e-mail messages it receives to another e-mail account.
Display Name	The name to appear in the e-mail From address. For example, Sales Department.
Domain	The domain name for the e-mail server.

Name	Description
Mailbox	The name of a mailbox on the e-mail server. If the Contact Center Multimedia server is in the same domain as the e-mail 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 e-mail 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 e-mail 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.
Password and Confirm	The password used to access the mailbox on the e-mail server. Type the password in the Confirm box to ensure accuracy.
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 e-mail server that delivers e-mail messages that leave the contact center.

Deleting a recipient mailbox

Before you begin

- Before you delete a mailbox, you must ensure that no e-mail 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.
- Log on to the Contact Center Manager Administration application.

About this task

Delete a recipient mailbox from your system if you no longer require it to monitor e-mail. Removing extra mailboxes saves space in your database.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **E-mail**.
3. Click **Recipient Addresses**.
4. Select an address from the recipient list and click **Delete**.
5. Click **Yes** to confirm to delete the recipient.

Updating the system default rule

Before you begin

- Ensure that you know the default settings for the system delivery failure rule:
  - use the e-mail default skillset, EM_Default_Skillset
  - use no automatic response
  - assign priority 3 (medium high)
- 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 e-mail messages.
- Configure the route points for the skillset you assign to the system default rule. For more information, see Configuring skillsets for e-mail on page 328.
- Log on to the Contact Center Manager Administration application.

About this task

Update the system default rule to ensure that an e-mail 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 e-mail 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

e-mail 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 e-mail. 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 6. For example, a call with priority 1 is handled before a call with priority 6.

Updating the system delivery failure rule

Before you begin

- Ensure that you are licensed to handle e-mail messages.
- Ensure that you know the default settings for the system delivery failure rule:
  - use the e-mail default skillset, EM_Default _Skillset
  - use keyword group delivery failure keywords
  - assign priority 6 (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 e-mail messages.
- Configure the route point for the skillset you plan to assign to the system delivery failure rule. See Configuring skillsets for e-mail on page 328.
- Log on to the Contact Center Manager Administration application.

About this task

Update the system delivery failure rule to ensure that any e-mail 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 e-mail 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 6. For example, a call with priority 1 is handled before a call with priority 6.
Will close contact	Select the check box to close the e-mail 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 e-mail contact open for review.

Creating or changing a keyword group

Before you begin

- Log on to the Contact Center Manager Administration application.

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 e-mail 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: # + - & | ! ( ) { } [ ] ^ “ ~ : and \. If you use any of these characters in your keywords, you receive an error message stating that the keyword contains invalid characters.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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. To allow close misspellings of the word, select the **Allow spelling inaccuracies** check box.
8. Specify the percent accuracy to configure.
9. Click **>**.
   The keyword or expression is added to the list, and the keyword group is created.
10. Repeat step 6 on page 338 through step 9 on page 338 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.

Name	Description
Keyword	A word, or string of characters, used to search the e-mail 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. Innaccuracies of 80% or 90% do not allow the error.

Deleting a keyword from a keyword group

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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**.
8. Click **Save**.

Deleting a keyword group

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Delete a keyword group. After you remove the keyword group, you cannot use it in any rule. Rules that use the deleted keyword group may not route the contact as expected.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **E-mail**.
3. Click **Keyword Groups**.
4. Select a keyword group from the **Keyword Groups** list.
5. Click **Delete**.
6. Click **OK**.

Creating or changing prepared responses

Before you begin

- Log on to the Contact Center Manager Administration application.

Important:

After creating an auto suggestion, you must add it to a rule group to make it available on the Agent Desktop.

Important:

The body of a prepared response is limited to 3900 characters.

Important:

You can include only images as inline attachments. The formats supported are .gif, .bmp, .jpg, and .png.

Important:

You can include inline attachments only by browsing to the image. The inline attachments are inserted where your cursor is placed in the body of the e-mail. You cannot paste inline attachments within an e-mail.

About this task

There are two types of prepared responses, auto response and auto suggestions. You can use automatic responses to send messages to a sender automatically. Suggested responses are provided to an agent for review and approval before the response is sent.

You must add a suggested response to a rule group, to make it available on the Agent Desktop.

Auto suggestions and auto responses support both standard and inline attachments. You can add inline attachments (only as images) such as company logos to the responses.

Agents can also place inline attachments (only as images) in e-mail messages.

Inline attachments display complete information within the body of the e-mail. 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 an automatic response or suggested response 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 e-mail contact (automatic response, or an automatic acknowledgement)
- 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 the Avaya Aura® Agent Desktop.

A password reminder and an out-of-office automatic response are configured by default. You cannot delete the default automatic responses.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **E-mail**.
3. Click **Prepared Responses**.
4. In the **Prepared Responses** table, click **New Response**.

   OR

   Select a response, and click **Edit**.
5. In the **Name** box, type 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 e-mail 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 e-mail message.
9. Optional: Click the **Image** icon.
   The Inline Attachment dialog box appears.
10. Optional: Beside the **Attachment** box, click **Add** to add attachments to the response.
11. Click **Save**.

Variable definitions

Name	Description
Name	The name of the automatic response. The name must be unique.
Type	Type of prepared response. An automatic response is sent when the e-mail message is received. An automatic suggestion is provided to the agents for selection and editing a response to the customer.
Subject	The subject of the prepared response used as an e-mail 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.
Attachment	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 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 e-mail.

Name	Description
Image Address (URL)	Type the url for the inline image that you want to include in the e-mail.
Alternate text	Type the alternative text for the image. Alternate text is what the customer views if their e-mail 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.

Procedure job aid

Use the following toolbar to format the prepared responses for your e-mail contacts.



Figure 7: Prepared response toolbar

Deleting prepared responses

About this task

Delete the prepared responses that are no longer used by agents in your contact center.

Procedure

1. In the left column of the **Multimedia Administrator**, click **E-mail**.
2. Click **Prepared Responses**.
3. Select an existing prepared response.
4. Click **Delete Response**.
5. Click **Yes** to confirm.

Removing attachments from prepared responses

Before you begin

- Log on to the Contact Center Manager Administration application.

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 e-mail.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
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. Under the **Attachments** box, click **Delete**.
7. Click **Save**.

Promoting suggested responses

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 e-mail addresses to particular skillsets.

Using a sender group in a rule is optional.

Sender groups support only asterisks (*) as a wildcard character when it is placed before the at symbol (@) in the e-mail address. You cannot use the wildcard characters at the end of a sender group address.

Avaya recommends that you have a maximum of 20 sender e-mail addresses in one sender group.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.

2. In the left column, 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 e-mail address.
7. If you know the user is in the contact database, start typing an e-mail address, and then click **Look up e-mail**.
   E-mail addresses that match the characters appear in the list.
8. Click **Add** to insert the e-mail address you looked up, or click **Add Freeform** to add your typed e-mail address to the sender group.
   This text box supports unicode language.
9. Repeat step 5 on page 346 through step 8 on page 346 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 e-mail 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 345.

About this task

Delete a sender group from your contact center if it is not required in the contact center.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **E-mail**.
3. Click **Sender Groups**.
4. Select the Sender Group you want to remove.
5. Click **Delete**.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **E-mail**.
3. Click **Sender Groups**.
4. Select a sender group from the list.
5. Click **Edit**.
6. Under **Edit Sender Group** box, select the e-mail address from the list.
7. Click **Remove**.
8. Click **Save**.

Creating or changing rules

Before you begin

- If you plan to use office hours for routing e-mail messages, configure your office hours. See Configuring office hours on page 308.
- Configure at least one e-mail skillset. See Configuring skillsets for e-mail on page 328.

- Create keyword groups, if required. See Creating or changing a keyword group on page 337.
- Configure prepared responses (automatic responses or suggestions), if required for the rule. See Creating or changing prepared responses on page 340.

About this task

Create or change a rule to route your e-mail contacts.

A rule is a mechanism for routing e-mail contacts. In your contact center, you receive e-mail 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 e-mail was received (office hours)
- determine who sent the e-mail (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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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. Click **Go**.
8. Configure the keyword match or sender group to use.
9. Repeat step 5 on page 348 to step 7 on page 348 to select a maximum of five criteria for the rule.
10. Click **OK**.
11. Under **Current Search Criteria**, choose the weighting for each criterion. The total weighting must add up to 100 percent.
12. Under **Current Search Criteria Summary**, click the blue text to view the details of each criterion you configure.
13. Click **Next**.

14. To select an automatic response for the rule, under **Available Auto-Responses**, select the configured automatic response, and then click **>**.
15. 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.
16. Click **Next**.
17. In the **General Settings** area, in the **Name** box, type a name for the rule.
18. In the **Priority** box, select the priority to assign to the contact.
19. In the **Skillset** box, select the skillset to apply for the rule.
20. If you want to apply the office hours to the e-mail message, click **Will use Office hours**.
21. To close the contact, click **Will Close Contact**.
22. Click **Save**.

Variable definitions

Name	Description
New Criterion	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 e-mail address from which the e-mail message is received. Choose a maximum of five criteria for each rule.
Available Auto Response	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 Suggest	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.

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 6.
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.

Enabling a rule

About this task

Rules can be enabled within a rule group.

Procedure

1. In the left column of the **Multimedia Administrator**, click **E-mail**.
2. Click **Rule Groups**.
3. Select a disabled rule.
4. Under **Rules**, click the check mark (√) button.
5. 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. In the left column of the **Multimedia Administrator**, click **E-mail**.
2. Click **Rule Groups**.
3. Select an enabled rule.
4. Under **Rules**, click the cross (**X**) button.
5. Click **Save**.

Deleting a rule

Before you begin

- Create a rule.
- Log on to the Contact Center Manager Administration application.

About this task

Permanently delete a rule. After you delete the rule, you cannot use the rule for routing e-mail 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **E-mail**.
3. Click **Rule Groups**.
4. Under **Rules**, select the name of the rule to delete.
5. Click the minus sign (**—**) button.

6. Click **Yes** to confirm.
7. Click **Save**.

Creating or changing rule groups

Before you begin

- Log on to the Contact Center Manager Administration application.

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 e-mail (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 e-mail 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 e-mail message.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 e-mail 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 e-mail 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 the e-mail settings

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Configure the following e-mail settings for e-mail messages entering and leaving your designated contact center mailboxes:

- how frequently you scan the e-mail server for new messages
- the location in which attachments are stored
- automatic numbering of e-mail 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **E-mail**.
3. Click **General Settings**.
4. To configure a mailbox scan interval, under **Mailbox Scan Interval**, in the **Interval** box, type the time in minutes.

5. To change the attachment file locations, under **Attachment Files**, type the new paths for the inbound and outbound URL and shared folders into the fields provided.
6. To include the customer ID or contact ID in a number for the outgoing e-mail message numbering, under **Message Properties**, select the **Customer ID** check box, the **Contact ID** check box, or both.
7. To include the e-mail message body in the keyword search, select the **Include email body in keyword search** check box.
8. Click **Save**.

Variable definitions

Name	Description
Interval	The interval between mailbox scans to check for new incoming e-mail messages. You can specify minutes and seconds between each scan.
Inbound Url	The uniform resource locator (URL) that shows the location of the inbound e-mail attachments.
Inbound Share	The path of the shared folder on the Contact Center Multimedia server in which the inbound e-mail attachments are stored.
Outbound Url	The uniform resource locator (URL) that shows the location of the outbound e-mail attachments.
Outbound Share	The path of the shared folder on the Contact Center Multimedia server in which the outbound e-mail attachments are stored.
Autonumber outgoing e-mail	Select the check box to number the e-mail message automatically with either the customer ID, the contact ID, or both. The number appears in the subject of the message for identification.
Include e-mail body in keyword search	Select the check box to enable a keyword search in both the subject and the body of the e-mail message.
Search for first characters	Specify the number of characters in the content of the body of the e-mail message

Name	Description
	that you search for keywords if you enabled the keyword search in the body of the e-mail message.

Changing the character encoding for outgoing and incoming e-mail

Before you begin

- Avaya recommends that only contact centers in Europe use Latin-9 encoding.
- Log on to the Contact Center Manager Administration application.

About this task

Change the character encoding of outgoing e-mail to reply to an e-mail message by using the same character set as the inbound e-mail. For example, if an e-mail 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 e-mail 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 e-mail 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 e-mail 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **E-mail**.
3. Click **General Settings**.
4. In the **Encoding** list, select the type of character encoding to use.
5. To use Latin-9 encoding for replies, select the **Reply to Latin 1 as Latin 9** check box.
6. Click **Save**.
7. On the **Start** menu of the Contact Center Multimedia server, click **All Programs** > **Administrative Tools** > **Services**.
8. Right-click **CCMM Email Manager.**
9. Click **Restart**.

10. Close the Services window.

Selecting the outgoing e-mail address

Before you begin

- Configure the e-mail mailbox from which to send outbound e-mail messages. See Creating or changing a recipient mailbox on page 329.
- Log on to the Contact Center Manager Administration application.

About this task

You can send e-mail messages from the e-mail address to which the original message was sent or from a general e-mail address in the contact center.

You can choose the response e-mail address based on a skillset.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 e-mail 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 email address**, and then select the e-mail address for the outgoing e-mail.
8. To send customer responses from the address that the customer used, click **Respond to Customer Contacts with the Recipient address of the original email, and send Agent-Initiated Contacts from this address**.
9. Click **Save**.

Barring e-mail addresses

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Configure Contact Center Multimedia to block certain e-mail addresses. When you bar an e-mail address, automatic replies, and agent e-mail messages are not sent to the barred address.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **E-mail**.
3. Click **Outgoing E-mail**.
4. Click the **Barred Outgoing Addresses** tab.
5. Click **New**.

   OR

   Select an existing barred e-mail address, and then click **Edit**.
6. In the **Address** box, type the e-mail address to block.
7. Click **Save**.
   The address appears in the list of Barred Addresses.

Deleting a barred e-mail address

Before you begin

- Ensure that removing a barred address does not violate local governing for do-not-call lists.
- Log on to the Contact Center Manager Administration application.

About this task

Remove a blocked e-mail address from the barred e-mail address list.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.

2. In the left column, click **E-mail**.
3. Click **Outgoing E-mail**.
4. Click the **Barred Outgoing Addresses** tab.
5. Select a barred e-mail address from the list provided.
6. Click **Delete**.
7. Click **OK** to confirm the deletion.

Configuring Microsoft Exchange for sending outgoing e-mail

Before you begin

- Ensure that you use Microsoft Exchange on your e-mail server.
- Log on to the Contact Center Manager Administration application.

About this task

If Microsoft Exchange 2007 or later is installed on your e-mail server, configure it to send outgoing e-mail from Avaya Aura® Agent Desktop.

If you use Microsoft Exchange 2003, skip this procedure.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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.

Enabling SSL on the Email Manager

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 unsecure.

About this task

Enable Secure Sockets Layer (SSL) on the Email Manager. Contact Center Multimedia supports Secure Sockets Layer (SSL) to protect data traveling between the e-mail server and the Contact Center Multimedia server.

Although SMTP is secure, when e-mail traverses the Internet, it becomes unsecure. Implementations of secure SMTP vary as does the port number. For more information, see the documentation for your e-mail server.

The following error may occur:

```
EmailManager.log file javax.net.ssl.SSLHandshakeException: Could not
find trusted certificate.
```

This message indicates that the target mail server SSL certificate was signed with a certificate from a signing authority that is not trusted or you that are using a test certificate must enable SMTP Authentication on your e-mail server.

Note:

Avaya Aura® Contact Center supports monitored mailboxes distributed across several e-mail servers. If you want to use POP3 or SMTP over SSL, you must enable SSL on all monitored mailboxes. Mixed SSL and non-SSL enabled e-mail servers are not supported.

Note:

The CCMM dashboard application does not support SSL. After you enable SSL on the Email Manager, the CCMM Dashboard falsely indicates that CCMM failed to connect to the configured mailboxes.

Procedure

1. Open the mailservice.properties file. The mailservice.properties file is in X:\Avaya \Contact Center\Multimedia Server\Server Applications\EMAIL; X is the drive on which you installed your Multimedia server software.
2. Copy the following lines into mailservice.properties file.

   ```
   mail.pop3.socketFactory.class=javax.net.ssl.SSLSocketFactory
   mail.pop3.socketFactory.fallback=false
   mail.pop3.socketFactory.port=995
   ```

3. In the Contact Center Manager Administration application, click **Multimedia**.
4. In the left column, click **General Administration**.
5. Click **Server Settings**.
6. In the Server Settings window, select **Inbound POP3 Server**.
7. Click **Edit**.
8. In the **Primary Hostname** box, type the name of the server that receives e-mail messages.
9. In the **Port Number** box, type the standard port number (995) for the e-mail server.
10. In the **Secondary Hostname** box, if you have a backup e-mail server, provide a host name for the backup server.
11. Click **Save**.

12. Copy the following lines into mailservice.properties file.

```
mail.smtp.socketFactory.class=javax.net.ssl.SSLSocketFactory
mail.smtp.socketFactory.fallback=false
mail.smtp.socketFactory.port=25
```

13. Use Java keytool to enable trust for a signing authorities certificate. By default, Java application SSL implementations automatically trust many of the major certificate authorities such as Verisign or Thawte. However, if you use a test certificate you must add the following text to C:\Program Files (x86)\Java\jre6\lib\security\cacerts:

```
keytool -import -alias mycacert -file mycacert.cer -
keystore
```

14. When you are prompted for a keystore password, use the default installation password for the JRE trust keystore, `changeit`.
15. After the certificate details are printed, you are prompted to Trust this certificate.
16. Type `y` or `yes`, and then press `Enter` to update the keystore.

    The file appears as follows:

```
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
```

17. Enter the keystore password `changeit`.
18. Restart the **Email Manager** service.
19. To change the default password for security reasons, type the following command and you are prompted for a new password:

```
keytool -storepasswd -new changeit -keystore
C:\Program Files (x86)\Java\jre6\lib\security\cacerts
```

Enabling SMTP Authentication on your e-mail server

About this task

Enable SMTP authentication for Microsoft Exchange Server 2003 or Microsoft Exchange Server 2007. SMTP Authentication is a mechanism to restrict nonauthenticated clients from sending e-mail messages outside your organization. Agents who want to send external e-mail

messages must provide their logon credentials to the e-mail server before their e-mail is relayed. Failure to authenticate leads to an immediate message from the e-mail server indicating that sending the e-mail is prohibited or a later nondelivery report e-mail. 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 e-mail 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 e-mail server.

After a successful logon, you can send an e-mail 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 e-mail 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 e-mail message using the DATA command:

   ```
   DATA
   354 Send data. End with CRLF.CRLF
   ```

6. Conclude the e-mail message by typing <ENTER> . <ENTER>

   The e-mail message is sent.

   ```
   250 OK
   ```

7. If the SMTP Authentication is enabled, you must reconnect to your e-mail 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 e-mail mailbox account.

11. Confirm the user name and password.

Chapter 42: Voice mail configuration

In the contact center, the recipient mailboxes are polled for incoming voice mail messages. A voice mail server forwards voice mail messages to an e-mail 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.

This chapter contains the configuration steps for the voice mail recipient mailbox and routing voice mail contacts.

Prerequisites for voice mail configuration

- Ensure that you are licensed for e-mail contacts.
- Log on to the Contact Center Manager Administration application. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Configuring a route point for a voice mail skillset on page 366
- Adding a voice mail server on page 367
- Updating a voice mail server on page 367
- Deleting a voice mail server on page 368

- Adding a voice mail mailbox on page 368
- Updating a voice mail mailbox on page 370
- Deleting a voice mail mailbox on page 371
- Updating the voice mail system default rule on page 372
- Updating the voice mail system delivery failure rule on page 373

Configuring a route point for a voice mail skillset

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Add the voice mail server for your Contact Center Multimedia server as per your requirement.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Update the voice mail server for your Contact Center Multimedia server as per your requirement.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Voice Mail**.
3. Click **Mailbox Configuration**.
4. Click **Voice Mail Server**.

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

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Delete the voice mail server for your Contact Center Multimedia server if it is no longer required.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Voice Mail**.
3. Click **Mailbox Configuration**.
4. Click **Voice Mail Server**.
5. In the Voice Mail Server Configuration window, click **Delete**.
   A warning box appears.
6. Click **OK** to confirm the server deletion.
7. Click **Close**.

Adding a voice mail mailbox

Before you begin

- Configure a skillset for a voice mail contact.
- Log on to the Contact Center Manager Administration application.

Important:

You must configure the voice mail server, Avaya CallPilot®, the e-mail 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Voice Mail**.
3. Click **Mailbox Configuration**.
4. Click **Add**.
5. On the **Mailbox** tab, select the **POP3 Server** for your inbound mailbox.
6. In the **Mailbox** box, type the mailbox name.
7. In the **Domain** box, type the mailbox domain.
8. In the **Password** and **Confirm** boxes, type and retype the password to access the mailbox.
9. In the **Skillset** box, choose a configured skillset for routing the voice mail contacts.
10. In the **Contact Priority** box, choose a priority for voice mail contacts received in this mailbox.
11. Click the **Sender Address** tab.
12. Select **Use full sender address** or **Parse sender address for CLID**.
13. If you select **Parse sender address for CLID**, then in the **Leading Characters to Remove** box, type the characters that you must not dial when making the outgoing callback.
14. Click **Save**.

Variable definitions

Name	Description
POP3 Server	The name of the e-mail server that handles e-mail messages entering the contact center.

Name	Description
Mailbox	Name of the mailbox on the e-mail server that is polled for new incoming e-mail messages.
Domain	The domain name for the e-mail server.
Password	The password used to access the mailbox on the e-mail server. Type the password in the Confirm Password box to ensure accuracy.
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.
- Log on to the Contact Center Manager Administration application.

About this task

Update the properties of the voice mail mailbox, as per your requirements.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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.
- Log on to the Contact Center Manager Administration application.

About this task

Delete a voice mail mailbox, if it is no longer required.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Voice Mail**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.
   A warning box appears.
6. Click **OK** to confirm the deletion.
7. Click **Close**.

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 (medium high)
- 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 366.
- Log on to the Contact Center Manager Administration application.

About this task

Update the voice mail system default rule to ensure that e-mail messages received with voice mail attachments are routed to an agent if no other rule associated to the recipient mailbox routes the e-mail message.

The system default rule is used in every rule group configured in Contact Center Multimedia.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 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 the voice mail system delivery failure rule

Before you begin

- Ensure that you are licensed to handle e-mail 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 6 (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 366.
- Log on to the Contact Center Manager Administration application.

About this task

Update the voice mail system delivery failure rule to ensure that any e-mail 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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, check 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 e-mail 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 6. For example, a call with priority 1 is handled before a call with priority 6.

Name	Description
Will close contact	Select the check box to close the e-mail 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 e-mail contact open for review.

Chapter 43: Scanned document configuration

In the contact center, the recipient mailboxes are polled for incoming scanned documents. A server forwards scanned documents to an e-mail 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.

This chapter contains the configuration steps for the recipient mailbox that receives scanned documents.

Prerequisites for scanned document configuration

- Ensure that you are licensed for e-mail contacts.
- Log on to the Contact Center Manager Administration application. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Configuring a route point for a scanned document skillset on page 378
- Adding a document imaging server on page 379
- Updating a document imaging server on page 379

- Deleting a document imaging server on page 380
- Adding a scanned document mailbox on page 381
- Updating a scanned document mailbox on page 382
- Deleting a scanned document mailbox on page 383
- Configuring a scanned document reply mailbox on page 383
- Deleting a scanned document reply mailbox on page 385
- Updating the scanned documents system default rule on page 385
- Updating the scanned documents system delivery failure rule on page 386

Configuring a route point for a scanned document skillset

Before you begin

- Log on to the Contact Center Manager Administration application.

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. Click **Multimedia**.
2. In the left column, 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

Name	Description
	a script on the Contact Center Manager Server.

Adding a document imaging server

Before you begin

• Log on to the Contact Center Manager Administration application.

About this task

Add the document imaging server for your Contact Center Multimedia server as per your requirement.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Scanned Documents**.
3. Click **Mailbox Configuration**.
4. Click **Document Imaging Server**.
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

Before you begin

• Log on to the Contact Center Manager Administration application.

About this task

Update the document imaging server for your Contact Center Multimedia server as per your requirement.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.

2. In the left column, select **Scanned Documents**.
3. Click **Mailbox Configuration**.
4. Click **Document Imaging Server**.
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

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Delete the document imaging server for your Contact Center Multimedia server if it is no longer required.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Scanned Documents**.
3. Click **Mailbox Configuration**.
4. Click **Document Imaging Server**.
5. In the Document Server Configuration window, select the server you are updating and click **Delete**.
6. Click **OK** to confirm the deletion.
7. Click **Close**.

Adding a scanned document mailbox

Before you begin

- Configure a skillset for a scanned document.
- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Scanned Document**.
3. Click **Mailbox Configuration**.
4. Click **Add**.
5. On the **Mailbox** tab, select the **POP3 Server** for your inbound mailbox.
6. In the **Mailbox** box, type the mailbox name.
7. In the **Domain** box, type the mailbox domain.
8. In the **Password** and **Confirm** boxes, type and retype the password to access the mailbox.
9. In the **Skillset** box, choose a configured skillset for routing the contact.
10. In the **Contact Priority** box, choose a priority for contacts received in this mailbox.
11. Click **Save**.

Variable definitions

Name	Description
POP3 Server	The name of the e-mail server that handles e-mail messages entering the contact center.

Name	Description
Mailbox	Name of the mailbox on the e-mail server that is polled for new incoming e-mail messages.
Domain	The domain name for the e-mail server.
Password	The password used to access the mailbox on the e-mail server. Type the password in the Confirm box to ensure accuracy.
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.
- Log on to the Contact Center Manager Administration application.

About this task

Update the properties of the scanned document mailbox, as per your requirements.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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.
- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Scanned Document**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.
6. Click **OK** to confirm the deletion.
7. Click **Close**.

Configuring a scanned document reply mailbox

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 e-mail 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 e-mail server domain.
9. In the **Password** and **Confirm** boxes, type and retype the e-mail 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 e-mail server that handles e-mail messages leaving the contact center.
Mailbox	Name of the mailbox on the e-mail server polled for e-mail messages.
Domain	The domain name for the e-mail server.

Name	Description
Password	The password used to access the mailbox on the e-mail server. Type the password in the Confirm box to ensure accuracy.
Use Alternative username for SMTP Authentication	If SMTP authentication is required for your outbound e-mail server, select the user name for the authentication.

Deleting a scanned document reply mailbox

Before you begin

- Log on to the Contact Center Manager Administration application.

Important:

A scanned document reply mailbox cannot be deleted if it is currently assigned to a skillset.

About this task

Delete a scanned document reply mailbox, if it is no longer required.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Scanned Document**.
3. Click **Reply Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.
6. Click **OK** to confirm the deletion.
7. Click **Close**.

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 (medium high)

- 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 378.
- Log on to the Contact Center Manager Administration application.

About this task

Update the scanned documents system default rule to ensure that e-mail messages received with scanned document attachments are routed to an agent if no other rule associated to the recipient mailbox routes the e-mail message.

The system default rule is used in every rule group configured in Contact Center Multimedia.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 e-mail 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 6 (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 378.
- Log on to the Contact Center Manager Administration application.

About this task

Update the scanned documents system delivery failure rule to ensure that any e-mail 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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, check the **Will close contact** check box.
7. Click **Save**.

Chapter 44: Fax configuration

In the contact center, the recipient mailboxes are polled for incoming fax messages. A fax server forwards messages to an e-mail 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.

This chapter contains the configuration steps for the fax recipient mailbox.

Prerequisites for fax configuration

- Ensure that you are licensed for e-mail contacts.
- Log on to the Contact Center Manager Administration application. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Configuring a route point for a fax skillset on page 390
- Adding a fax server on page 391
- Updating a fax server on page 391
- Deleting a fax server on page 392
- Adding a fax mailbox on page 392

- Updating a fax mailbox on page 394
- Deleting a fax mailbox on page 395
- Configuring a fax reply mailbox on page 395
- Deleting a fax reply mailbox on page 397
- Updating the fax system default rule on page 397
- Updating the fax system delivery failure rule on page 398

Configuring a route point for a fax skillset

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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

Before you begin

• Log on to the Contact Center Manager Administration application.

About this task

Add the fax server for your Contact Center Multimedia server as per your requirement.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Fax**.
3. Click **Mailbox Configuration**.
4. Click **Fax Server**.
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

Before you begin

• Log on to the Contact Center Manager Administration application.

About this task

Update the fax server for your Contact Center Multimedia server as per your requirement.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Fax**.
3. Click **Mailbox Configuration**.
4. Click **Fax Server**.
5. In the Fax Server Configuration window, click **Edit**.

6. Change the properties of your fax server.
7. Click **Save**.

Deleting a fax server

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Delete the fax server for your Contact Center Multimedia server if it is no longer required.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Fax**.
3. Click **Mailbox Configuration**.
4. Click **Fax Server**.
5. In the Fax Server Configuration window, click **Delete**.
6. Click **OK** to confirm the deletion.
7. Click **Close**.

Adding a fax mailbox

Before you begin

- Configure a skillset for a fax contact.
- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Fax**.
3. Click **Mailbox Configuration**.
4. Click **Add**.
5. On the **Mailbox** tab, select the **POP3 Server** for your inbound mailbox.
6. In the **Mailbox** box, type the mailbox name.
7. In the **Domain** box, type the mailbox domain.
8. In the **Password** and **Confirm** boxes, type and retype the password to access the mailbox.
9. In the **Skillset** box, choose a configured skillset for routing the contacts.
10. In the **Contact Priority** box, choose a priority for contacts received in this mailbox.
11. Click the **Sender Address** tab.
12. Select **Use full sender address** or **Parse sender address for CLID**.
13. If you select **Parse sender address for CLID**, in the **Leading Characters to Remove** box, type the characters that you must not dial when making the outgoing callback.
14. Click **Save**.

Variable definitions

Name	Description
POP3 Server	The name of the e-mail server that handles e-mail messages entering the contact center.
Mailbox	Name of the mailbox on the e-mail server that is polled for new incoming e-mail messages.
Domain	The domain name for the e-mail server.
Password	The password used to access the mailbox on the e-mail server. Type the password in the Confirm box to ensure accuracy.

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.
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.
- Log on to the Contact Center Manager Administration application.

About this task

Update the properties of the fax mailbox, as per your requirements.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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.
- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Fax**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.
6. Click **OK** to confirm the deletion.
7. Click **Close**.

Configuring a fax reply mailbox

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 e-mail 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 e-mail server domain.
9. In the **Password** and **Confirm** boxes, type the e-mail 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 e-mail server that handles e-mail messages leaving the contact center.
Mailbox	Name of the mailbox on the e-mail server polled for e-mail messages.
Domain	The domain name for the e-mail server.
Password	The password used to access the mailbox on the e-mail server. Type the password in the Confirm box to ensure accuracy.

Name	Description
Use Alternative username for SMTP Authentication	If SMTP authentication is required for your outbound e-mail server, select the user name for the authentication.

Deleting a fax reply mailbox

Before you begin

- Log on to the Contact Center Manager Administration application.

Important:

A fax reply mailbox cannot be deleted if it is currently assigned to a skillset.

About this task

Delete a fax reply mailbox, if it is no longer required.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Fax**.
3. Click **Reply Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.
6. Click **OK** to confirm the deletion.
7. Click **Close**.

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 (medium high)
- 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 390.
- Log on to the Contact Center Manager Administration application.

About this task

Update the fax system default rule to ensure that e-mail messages received with fax attachments are routed to an agent if no other rule associated to the recipient mailbox routes the e-mail message.

The system default rule is used in every rule group configured in Contact Center Multimedia.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 e-mail 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 6 (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 390.
- Log on to the Contact Center Manager Administration application.

About this task

Update the fax system delivery failure rule to ensure that any e-mail 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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, check the **Will close contact** check box.
7. Click **Save**.

Chapter 45: 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.

Prerequisites for instant message configuration

- Ensure that you have a license for instant messages.
- Log on to the Contact Center Manager Administration application. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Configuring welcome and disconnect messages on page 402
- Creating automatic phrases on page 403
- Deleting an automatic phrase on page 404
- Creating a page push URL on page 404
- Deleting a page push URL on page 405
- Adding an expert manually to Contact Center Multimedia on page 406
- Importing an expert from files to Contact Center Multimedia on page 406
- Searching for users in the Active Directory on page 407
- Importing an Active Directory user to Contact Center Multimedia on page 408
- Creating an expert group on page 409
- Deleting an expert group on page 410

- Adding experts to a skillset on page 411
- Deleting experts from a skillset on page 411

Configuring welcome and disconnect messages

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 200 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

Before you begin

- Log on to the Contact Center Manager Administration application.

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.

Ensure that you make the name of the automatic phrase descriptive to assist the agents using the Agent Desktop.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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**.

Deleting an automatic phrase

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **IM**.
3. Click **Auto Phrases**.
4. In the **Auto Phrases** dialog box, select the skillset to change the phrases.

   OR

   Select **All Skillsets**.
5. Click **Edit**.
6. In the **Phrases in Group** box, select the automatic phrase to delete.
7. Click **Remove**.
8. Click **Save**.

Creating a page push URL

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 Web site 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

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Delete a page push URL to remove it from the list of pages the agent can push to customers during an instant message contact.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **IM**.
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**.
   The Edit Push Page URL dialog box appears.

6. In the **URLs in Group** box, select the URL to delete.
7. Click **Remove**.
8. Click **Save**.

Adding an expert manually to Contact Center Multimedia

Before you begin

• Log on to the Contact Center Manager Administration application.

About this task

To add an agent to the Experts list, you can manually add an agent to CCMM.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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

Before you begin

• Log on to the Contact Center Manager Administration application.

About this task

To add an agent to the Experts list, you can import an agent from files to CCMM.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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.

Searching for users in the Active Directory

Before you begin

- Log on to the Contact Center Manager Administration application.

Important:

Searching for users in Active Directory is possible only when presence is provided by Office Communications Server.

About this task

You can search for users in the Active Directory, in order to import users to CCMM.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **IM**.
3. Click **Import Experts**.
4. In the **Domain Name** field, enter the domain or IPv4 address based on which you can search for users.

5. In the **Port** field, enter the active directory port.
6. In the **Username Filter** field, enter the wildcards with which to search. For example, enter all or part of the name of the user you are searching for. Enter * to view a list of all SIP-enabled users.
7. In the **Search Base** field, specify the preciseness of the Active Directory search. For example, in a large enterprise of tens of thousand of people, it may not be 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.
8. Configure the search options.
9. Enter the user name and password to connect to the domain.
10. Click **Search**.

Importing an Active Directory user to Contact Center Multimedia

Before you begin

- Log on to the Contact Center Manager Administration application.

Important:

Importing Active Directory users to CCMM is possible only when presence is provided by Office Communications Server.

About this task

To add an agent to the Experts list, you can import an agent to CCMM from the Active Directory.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **IM**.
3. Click **Import Experts**.
4. Click the **Active Directory** tab.
5. Search the Active Directory for SIP-enabled users. See Searching for users in the Active Directory on page 407.
6. In the **Active Directory** users list, select the users to import.
7. Click **>**.
   The agent name appears in the Experts list.

8. Optional: Once the experts have been imported into the **CC Experts List** you can enter values in the user's custom fields. Expand the user in the list by clicking the **+** adjacent to the user and enter the custom field values.
9. Repeat as necessary.
10. Click **Save**.

Creating an expert group

Before you begin

- Log on to CCMM.
- 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 5 on page 409 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.

Deleting an expert group

Before you begin

- Log on to CCMM.
- Set up an expert group.

About this task

Delete an expert group, if it is no longer required.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **IM**.
3. Click **Expert Groups**.
4. Select the group from the grid and click **Delete**.

Adding experts to a skillset

Before you begin

- Log on to CCMM.
- Skillsets must be configured.

About this task

You can add experts to a skillset associated group.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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**.

Deleting experts from a skillset

Before you begin

- Log on to CCMM.
- Expert must be associated with the skillset.

About this task

If an expert is no longer available, remove the agent name from a skillset associated group.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **IM**.
3. Click **Skillsets**.

4. Select the skillset from the list and click **Edit**.
5. Select the experts you want to remove from the second list under **Skillset Experts**.
6. Select the expert and click **<** to remove the experts from the skillset.
7. Click **Save**.

Chapter 46: Short Message Service configuration

In the contact center, the recipient mailboxes are polled for incoming Short Message Service (SMS) messages. A server forwards the SMS messages to an e-mail 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.

This chapter contains the configuration steps for the SMS recipient mailbox.

Prerequisites for SMS configuration

- Ensure that you are licensed for e-mail contacts.
- Log on to the Contact Center Manager Administration application. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Configuring a route point for an SMS skillset on page 414
- Adding an SMS Gateway on page 415
- Updating an SMS Gateway on page 415
- Deleting an SMS Gateway on page 416

- Adding an SMS mailbox on page 416
- Updating an SMS mailbox on page 418
- Deleting an SMS mailbox on page 419
- Configuring an SMS reply mailbox on page 419
- Deleting an SMS reply mailbox on page 421
- Updating the SMS system default rule on page 421
- Updating the SMS system delivery failure rule on page 422

Configuring a route point for an SMS skillset

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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

Before you begin

• Log on to the Contact Center Manager Administration application.

About this task

Add the SMS server for your Contact Center Multimedia server as per your requirement.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Click **SMS Gateway**.
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

Before you begin

• Log on to the Contact Center Manager Administration application.

About this task

Update the SMS server for your Contact Center Multimedia server as per your requirement.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Click **SMS Gateway**.
5. In the SMS Gateway Configuration window, click **Edit**.
6. Change the properties of your SMS server.

7. Click **Save**.

Deleting an SMS Gateway

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Delete the SMS server for your Contact Center Multimedia server if it is no longer required.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Click **SMS Gateway**.
5. In the SMS Gateway Configuration window, select the SMS gateway you are deleting and click **Delete**.
6. Click **OK** to confirm the deletion.
7. Click **Close**.

Adding an SMS mailbox

Before you begin

- Configure a skillset for an SMS contact.
- Log on to the Contact Center Manager Administration application.

About this task

Add an SMS mailbox to the multimedia configuration for receiving SMS messages in an e-mail 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Click **Add**.
5. On the **Mailbox** tab, select the **POP3 Server** for your inbound mailbox.
6. In the **Mailbox** box, type the mailbox name.
7. In the **Domain** box, type the mailbox domain.
8. In the **Password** and **Confirm** boxes, type and retype the password to access the mailbox.
9. In the **Skillset** box, choose a configured skillset for routing the contacts.
10. In the **Contact Priority** box, choose a priority for contacts received in this mailbox.
11. Click the **Sender Address** tab.
12. Select **Use full sender address** or **Parse sender address for CLID**.
13. If you select **Parse sender address for CLID**, in the **Leading Characters to Remove** box, type the characters that you must not dial when making the outgoing callback.
14. Click **Save**.

Variable definitions

Name	Description
POP3 Server	The name of the e-mail server that handles e-mail messages entering the contact center.
Mailbox	Name of the mailbox on the e-mail server that is polled for new incoming e-mail messages.
Domain	The domain name for the e-mail server.
Password	The password used to access the mailbox on the e-mail server. Type the password in the Confirm Password box to ensure accuracy.

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 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.
- Log on to the Contact Center Manager Administration application.

About this task

Update the properties of the SMS mailbox, as per your requirements.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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.
- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Text Messaging (SMS)**.
3. Click **Mailbox Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.
6. Click **OK** to confirm the deletion.
7. Click **Close**.

Configuring an SMS reply mailbox

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 e-mail 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 e-mail server domain.
9. In the **Password** and **Confirm** boxes, type the e-mail 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 e-mail server that handles e-mail messages leaving the contact center.
Mailbox	Name of the mailbox on the e-mail server polled for e-mail messages.
Domain	The domain name for the e-mail server.

Name	Description
Password	The password used to access the mailbox on the e-mail server. Type the password in the Confirm Password box to ensure accuracy.
Use Alternative username for SMTP Authentication	If SMTP authentication is required for your outbound e-mail server, select the user name for the authentication.

Deleting an SMS reply mailbox

Before you begin

• Log on to the Contact Center Manager Administration application.

About this task

Delete an SMS reply mailbox, if it is no longer required.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Text Messaging (SMS)**.
3. Click **Reply Configuration**.
4. Select the mailbox to be deleted.
5. Click **Delete**.
6. Click **OK** to confirm the deletion.
7. Click **Close**.

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 (medium high)
• 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 414.
- Log on to the Contact Center Manager Administration application.

About this task

Update the SMS system default rule to ensure that e-mail messages received with SMS text are routed to an agent if no other rule associated to the recipient mailbox routes the e-mail message.

The system default rule is used in every rule group configured in Contact Center Multimedia.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 e-mail 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 6 (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 414.
- Log on to the Contact Center Manager Administration application.

About this task

Update the SMS system delivery failure rule to ensure that any e-mail 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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, check the **Will close contact** check box.
7. Click **Save**.

Chapter 47: Web communications configuration

The Contact Center Multimedia server supports text-based conversations between the customer and the agent by using Web communications text chat in an Avaya Communication Server 1000 environment. When customers initiate a Web communications contact, a list of skillsets determines the appropriate topic for the contact.

Before making any Web communications contacts, you must ensure the Web Communications server is configured.

To personalize the Web communications contacts, you can configure welcome messages for all contacts, and specialized messages for each skillset. You can also 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, 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.

The Web on hold URLs creates 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 Aura® 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.

Prerequisites for Web communications configuration

- Ensure that you have a license for Web communications.
- Log on to the Contact Center Manager Administration application. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Assigning a development Web server name on page 427
- Configuring welcome messages and text chat labels on page 428
- Configuring Web communications agent timers on page 429
- Configuring customer notification log on page 431
- Allowing anonymous Web communcations on page 432
- Enabling Web Communications transfer to a skillset on page 432
- Creating automatic phrases on page 433
- Deleting an automatic phrase on page 434
- Creating a page push URL on page 434
- Deleting a page push URL on page 435
- Creating Web On Hold URLs groups on page 436
- Changing the sequence of URLs in a Web On Hold URLs group on page 437
- Deleting a URL from a Web On Hold URL group on page 437
- Deleting a Web On Hold URLs group on page 438
- Creating Web On Hold comfort groups on page 439
- Changing the sequence of messages in a Web On Hold comfort group on page 440
- Deleting a message from a Web On Hold comfort group on page 440
- Deleting a Web On Hold comfort group on page 441
- Creating Web communications comfort groups on page 442
- Changing the sequence of messages in a Web communications comfort group on page 443
- Deleting a message from a Web communications comfort group on page 444
- Deleting a Web communications comfort group on page 444
- Configuring intrinsics for agent-supervisor observe and barge-in on page 445

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 Web site from a test computer to the production server, you must configure the external Web server name.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 Web site.
6. In the **Server Port** box, type the port number for the external Web server you use to develop your custom Web site.
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 Web site.
Server Port	The port number for the external Web server for your custom Web site.

Configuring welcome messages and text chat labels

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 200 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 First Name, Last Name, or both. 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 till 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, John). • 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, John 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, John). You can also type custom text to appear at the beginning of the agent responses. The maximum size of the label is 50 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 50 characters.

Configuring Web communications agent timers

Before you begin

• Log on to the Contact Center Manager Administration application.

About this task

Configure the contact timers for Web communications conversations in your Contact Center.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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.

Name	Description
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.

Configuring customer notification log

Before you begin

- Configure an outgoing e-mail address to use to send the log file to the customer.
- Log on to the Contact Center Manager Administration application.

About this task

Configure the customer notification log information to prepare to send an e-mail to the customer of the written conversation.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Web Comms**.
3. Click **Config**.
4. Under **Chat Conversation**, select **E-mail Chat Log to Customer**.
5. Click **Save**.

Allowing anonymous Web communcations

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Allow an anonymous customer to create a web chat and enter an e-mail address or phone number. The system then searches for a matching customer in the database and links this Web chat to that customer's history.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Web Comms**.
3. Click **Config**.
4. Under **Anonymous Chat**, Select the **Allow unauthenticated customer while chat threading** check box.
5. Click **Save**.

Enabling Web Communications transfer to a skillset

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Configure the Web Communications (WC) transfer to a skillset feature to allow agents to transfer a WC contact to a skillset.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Web Comms**.
3. Click **Config**.
4. Select the **Enable Transfer To Skillset** checkbox.

5. Click **Save**.

Creating automatic phrases

Before you begin

- Log on to the Contact Center Manager Administration application.

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.

Ensure the name of the automatic phrase is descriptive to assist the agents using the Agent Desktop.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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**.
8. Click **Save**.

Creating a page push URL

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 Web site 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

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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**.
8. Click **Save**.

Creating Web On Hold URLs groups

Before you begin

- Log on to the Contact Center Manager Administration application.

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 plug-ins needed to run multimedia files.

Avaya recommends that you use no more than 25 URLs in each Web-on-hold group.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 **Sequence** box, type a number, from 1 to 25 to indicate the URL sequence you are configuring.
10. In the **URL** box, type the URL to display on the customer's Web browser.
11. Click **Add**.

12. Repeat step 5 on page 436 to step 11 on page 436 to add all URLs to the current Web on hold group.
13. Click **Save**.

Changing the sequence of URLs in a Web On Hold URLs group

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Change the order in which Web pages in a Web on hold URL group appear to customers.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Web Comms**.
3. Click **Web On Hold**.
4. Click the **On Hold Urls** tab.
5. Select the **Tag** to change.
6. Click **Edit**.
7. In the **Sequence** box, type a number, from 1 to 25 to indicate the URL order in the sequence you are configuring.
8. Click **Save**.

Deleting a URL from a Web On Hold URL group

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Delete a URL from a Web on hold URL group if the URL is not available.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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**.
8. Click **Save**.

Deleting a Web On Hold URLs group

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Web Comms**.
3. Click **Web On Hold**.
4. Click the **On Hold Urls** tab.
5. Select the **Group** to delete.
6. Click **Delete**.
7. Click **Save**.

Creating Web On Hold comfort groups

Before you begin

- Log on to the Contact Center Manager Administration application.
- 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 312.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 8 on page 439 and step 9 on page 439 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**.

Changing the sequence of messages in a Web On Hold comfort group

Before you begin

- Log on to the Contact Center Manager Administration application.
- Set up a Web on hold 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 on hold comfort group appear to customers.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Web Comms**.
3. Click **Web On Hold**.
4. Click the **On Hold Comfort Groups** tab.
5. Under **Comfort Group**, select the comfort group to change.
6. Click **Edit**.
7. Under **Group Messages**, use the arrow keys to configure the sequence of messages.
8. Click **Save**.

Deleting a message from a Web On Hold comfort group

Before you begin

- Log on to the Contact Center Manager Administration application.
- 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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**.
9. Click **Save**.

Deleting a Web On Hold comfort group

Before you begin

- Log on to the Contact Center Manager Administration application.
- 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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**.

Creating Web communications comfort groups

Before you begin

- Log on to the Contact Center Manager Administration application.
- 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 314.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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 442 and step 9 on page 442 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

- Log on to the Contact Center Manager Administration application.
- 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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

- Log on to the Contact Center Manager Administration application.
- 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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**.
8. Click **Save**.

Deleting a Web communications comfort group

Before you begin

- Log on to the Contact Center Manager Administration application.
- 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Web Comms**.
3. Click **Comfort Messages**.
4. Under **Comfort Group**, select the **Group** to delete.
5. Click **Delete**.

Configuring intrinsics for agent-supervisor observe and barge-in

Before you begin

- Log on to the Contact Center Manager Administration application.

Important:

Each intrinsic type has a unique priority level. For example, Conversation Length and Customer Idle Time intrinsics cannot have the same priority level.

About this task

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 Aura® 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.

Threshold values can be set, using Contact Center Multimedia, for the following intrinsics:

- Conversation Length (seconds)
- Seconds since last message out
- Seconds since last message in
- Number of Agent Messages
- Unanswered Messages

You also use Contact Center Multimedia to assign a priority from 1 to 5 (where 1 indicates highest priority) to each of the intrinsics. The system uses the threshold and priority values set

to sequence the aforementioned Web Communications contacts in a list. Contacts which require urgent attention appear at the top of this list.

The system flags a contact as requiring possible attention, if the value exceeds any of the defined thresholds. If the system flags more than one contact, then these contacts are sequenced based on a weighting. The system calculates these weighting using the priority of the intrinsic with exceeded thresholds. A higher weighting is given to intrinsics that have a higher priority.

For example, if contact A has exceeded the threshold for intrinsics of priority 1 and priority 2, and contact B has exceeded the threshold for intrinsics of priority 1 and priority 3, then contact A appears above contact B in the list.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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**, type a number, from 1 to 5, in the **Priority** box. Each intrinsic type has to have a unique priority level.

Chapter 48: Predictive Outbound administration

In a Predictive Outbound environment, the Pacing Algorithm forecasts the availability of an agent and originates calls on their behalf to maximize agent productivity. The Pacing Algorithm cannot “guess” the inbound call volume. After the Pacing Algorithm originates an outbound call on behalf of the agent, that agent cannot be assigned to a new arriving inbound call. Therefore, agents are exclusive to predictive outbound for a period of time. Agents cannot have an inbound and outbound skillset at the same time.

Predictive Outbound supports an advanced blending capability with which agents can move seamlessly between inbound and outbound queues as traffic levels change.

Predictive Outbound supports real-time blending of agents between inbound voice traffic and outbound dialing to react to changes in inbound call volumes. The solution offers highly flexible agent blending to blend some or all agents between inbound voice queues and outbound dialing.

For more information, see *Avaya Aura® Contact Center Predictive Outbound Fundamentals* (NN44400-106).

Prerequisites

- Ensure that you have administrator access rights.
- Log on to the Contact Center Manager Administration application. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Configuring predictive blending settings on page 448
- Configuring RTD Multicast settings on page 450
- Configuring predictive outbound agent scripts on page 451

Configuring predictive blending settings

Before you begin

- Create a blending threshold class. For more information, see *Avaya Aura® Contact Center Predictive Outbound Fundamentals* (NN44400-106).
- Log on to the Contact Center Manager Administration application.

About this task

The blending threshold class can include settings for multiple thresholds such as Average Wait Times, Agents Available, Abandoned Calls, and Service Levels. The next step is to identify from which threshold to trigger the blending capability.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Predictive Outbound**.
3. Click **General Settings**.
4. Under **Blending**, select the **Enable Blending** check box.
5. In the **Polling Interval** box, type the number of seconds between checks of the inbound skillsets with the blending template to move agents from the predictive outbound skillset.
6. In the **Reversal Polling Interval** box, type the number of seconds you want the blending service to check inbound skillsets and move agents to the predictive outbound skillset.
7. Click **Edit** to select a threshold to monitor.
8. From the **Threshold to Monitor** list, select a threshold class.

Important:

The blending service can monitor the following thresholds, except where noted.

Threshold class	Notes
%Service_Level_for_Ans_Calls	—
Average_Answer_Delay_S	—
%Service_Level_S	—
Calls Waiting	—
Total Wait Time	—
Max Wait Time	—

Threshold class	Notes
Expected Wait Time	—
Calls Answered	—
Calls Answd Aft Threshold	—
Total Answered Delay	—
Agent Available	—
Agent In Service	—
Longest Wait Since Last Call	Not available
Longest Wait Since Login	Not available
Agent Not Ready	—
Agent On This Skillset Call	—
Agent On DN Call	Not available
Agent Unavailable	—
Agent On Other Skillset Call	—
Agent On ACD-DN Call	Not available
Agent On NACD-DN Call	Not available
Call Offered	—
Call Abandon	—
Call Abandon Delay	—
Call Aband Delay Aft Threshold	—

9. In the **Number of agents to Inbound voice** box, type the number of agents to assign to the inbound skillset when the traffic exceeds the Level 2 threshold for the monitored threshold.
10. In the **Number of agents to Predictive Outbound** box, type the number of agents to return to the predictive outbound skillset when the traffic falls below the Level 1 threshold for the monitored threshold.
11. Click **Save**.

Variable definitions

Name	Description
Enable Blending	Enable (select the check box) or disable agent blending between predictive outbound and inbound skillsets.
Polling Interval	The frequency for which the inbound skillsets with the Blending_Template threshold assigned to are checked to determine if active predictive outbound agents are reassigned.
Reversal Polling Interval	The frequency for which the inbound skillsets with the Blending_Template threshold assigned to is checked to determine if agents are returned to outbound when the traffic is less than the Level 1 threshold for the monitored threshold.
Threshold to Monitor	Select the threshold to monitor from the list specified above.
Number of agents to Inbound voice	The number of active predictive outbound agents who are in standby priority on the inbound skillset and return to inbound when the traffic exceeds the Level 2 threshold for the monitored threshold.
Number of agents to Predictive Outbound	The number of transitioned agents that return to outbound in the reversal polling interval that is less than the Level 1 threshold for the monitored threshold.

Configuring RTD Multicast settings

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Configure the RTD Multicast settings for the real-time stream that the blending service monitors. These settings must match the multicast and port settings on Contact Center Manager Server.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Predictive Outbound**.
3. Click **General Settings**.
4. Under **RTD Multicast Configuration**, in the **Multicast IP** box, type the IP address to which Contact Center Manager Server sends real-time statistics.
5. In the **Port Number** box, type the port number that the blending service monitors to receive real-time statistics.
6. Click **Save**.

Configuring predictive outbound agent scripts

Before you begin

- Log on to the Contact Center Manager Administration application.
- Use a browser to verify the URL for the predictive outbound agent script.

About this task

After an agent receives an outbound contact, Agent Desktop presents a script associated with the campaign. The script contains details from the customer record and captures additional data during the call. Also, the script can serve as a workflow for the agent that branches to different pages depending on the progress of the call. These scripts are Web-based and are published on the CPSE2 Application Server.

Agent Desktop needs to know the base URL where the scripts are published. Each campaign script is in a subdirectory of the base URL.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Predictive Outbound**.
3. Click **General Settings**.
4. Under **Agent Script Configuration**, type the URL of the agent scripts.
5. Click **Save**.

Chapter 49: Agent Desktop configuration

The Contact Center Multimedia Administrator application has settings that you can use to configure properties in the Avaya Aura® Agent Desktop to help the agents access database information and work with contacts.

Perform the procedures in this chapter to configure the Agent Desktop settings.

Prerequisites for Agent Desktop configuration

- Log on to the Contact Center Manager Administration application. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Navigation

- Resetting an agent password on page 454
- Configuring agent access to contacts on page 455
- Controlling access to e-mail message text on page 455
- Creating or changing custom fields in Agent Desktop on page 456
- Deleting a custom field in Agent Desktop on page 456
- Configuring the active contact timer on page 457
- Configuring the callback timer on page 458
- Configuring the callback trunk access on page 458
- Specifying the attachment size on page 459
- Configuring Agent Desktop behavior on page 460
- Configuring the state of the Agent terminal on log off on page 461
- Configuring hotdesking on page 461
- Configuring hotdesking in a Citrix environment on page 462
- Creating or changing a closed reason on page 462
- Configuring default closed reasons on page 463
- Deleting a closed reason on page 464

- Configuring Screen Pops on page 465
- Enabling Customer History on Voice Contacts on page 466
- Configuring Advanced Settings on page 467

Resetting an agent password

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Reset an agent password if the agent forgets it or for any other reason.

If you only assign the password, you can use the default password. The default password is the same as the agent logon ID.

You can also choose the agent password.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **General Administration**.
3. Click **Agent Settings**.
4. Under **Edit Current Agents**, select the agent whose password to change or reset.
5. Under **Edit Agent Details**, click **Set Password** to choose the agent password.

   Note:

   To use the default password, clear the **Set Password** box.
6. Type the new password in the **New Password** and **Confirm Password** boxes.
7. Click **Save**.

Controlling access to e-mail message text

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Agents, by default, cannot edit text in an e-mail message. You can either enable particular agents or enable all agents to delete text from e-mail messages that enter the contact center.

For example, select this feature so agents can delete credit card information from an e-mail message to protect confidential customer information.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia.**
2. In the left column, click **General Administration.**
3. Click **Agent Settings.**
4. Select the **Enable Email Text Deletion For All Agents** check box, to enable all agents to delete text from e-mail messages.

   OR

   Click the agent, and under **Delete Enabled**, click the **Yes** option, to enable that agent to delete text from e-mail messages.
5. Click **Save**.

Configuring agent access to contacts

Before you begin

- Log on to the Contact Center Manager Administration application.

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.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.

2. In the left column, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. Under **Agent Skillset Partitioning**, select **Enable Partitioning**.

Creating or changing custom fields in Agent Desktop

Before you begin

- Log on to the Contact Center Manager Administration application.

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 e-mail address or phone numbers.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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.

Deleting a custom field in Agent Desktop

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Delete a custom field from the Agent Desktop when it is not required.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Agent Desktop Configuration**.
3. Click **Resources**.
4. Under **Current Custom Fields**, select a custom field.
5. Click **Delete**.
6. In the confirmation dialog box, click **OK**.

Configuring the active contact timer

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Configure the maximum amount of time that you want a multimedia contact to remain open on a desktop.

When this time expires, the contact remains open for a maximum of an hour more than the maximum open duration set in CCMM Administration. Agent Desktop force closes the contact three minutes before 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. Agent Desktop displays a final warning 3 minutes before the contact is force closed, with no option to continue.

The default time in the Contact Center Multimedia configuration is 1 hour (60 minutes).

Note:

If you are using Microsoft Office Communications Server (OCS) as your IM provider, the OCS server applies a maximum timeout of ten minutes which overrides this value (if it is greater than ten minutes). If there is no activity on the IM contact after ten minutes, OCS closes the contact.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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.

Configuring the callback timer

Before you begin

- Log on to the Contact Center Manager Administration application.

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.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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.

Configuring the callback trunk access

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Configure the callback trunk access to ensure that you can create a callback to the customer you work with in your contact. The customer can request a callback, and you can schedule callbacks.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. Under **Callback Trunk Access**, type the trunk access number in the **Trunk Access Code** box.

Specifying the attachment size

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

Specify the maximum size of the attachments that an agent can attach to an e-mail message.

Important:
The maximum file size set for attachments also applies to inline attachments.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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.

Configuring Agent Desktop behavior

Before you begin

- Log on to the Contact Center Manager Administration application.

Important:

Changes you make to the Agent Desktop configuration take effect only when agents restart Agent Desktop.

About this task

You can configure the Agent Desktop behavior to alert the agent when a new contact arrives. The behavior can be one or more of the following:

- Bring the Agent Desktop to the front.
- Make an audible alert.
- Give focus to the Agent Desktop.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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**, **Audible Alert**, or **Give focus**.

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

Name	Description
	warning sound and the toolbar flashes, but it is not brought to the front. • Audible alert: A sound is played on the computer when a contact is presented to the agent. • 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

Before you begin

• Log on to the Contact Center Manager Administration application.

About this task

Configure the agent terminal to be in idle or busy state when the agent logs off of the Agent Desktop.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. Under **Logoff Terminal State**, select **Idle** or **Busy**.

Configuring hotdesking

Before you begin

• Install Contact Center Multimedia or Agent Desktop. See *Avaya Aura® Contact Center Installation* (NN44400-311).

• Log on to the Contact Center Manager Administration application.

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

the Agent Desktop, they automatically map to the relevant terminal and addresses without user intervention.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **Agent Desktop Configuration**.
3. Select **General Settings**.
4. Under **Hot Desking**, select the **Enabled** check box.

Configuring hotdesking in a Citrix environment

Before you begin

- Log on to the Contact Center Manager Administration application.

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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Agent Desktop Configuration**.
3. Click **General Settings**.
4. Under **Hot Desking**, select the **Prompt for WorkStation** check box.

Creating or changing a closed reason

Before you begin

- Log on to the Contact Center Manager Administration application.

Important:

You cannot modify a default closed reason code.

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 463.

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.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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.

Configuring default closed reasons

Before you begin

- Create a closed reason. See Creating or changing a closed reason on page 462.

About this task

You can specify a default closed reason for each contact type (e-mail, 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.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Agent Desktop Configuration**.
3. Click **Default Closed Reasons**.

4. Under **Default Closed Reasons** box, beside **E-mail**, select the configured closed reason to apply to e-mail message contacts by default.
5. Under **Default Closed Reasons** box, beside **Fax**, select the configured closed reason to apply to e-mail message contacts by default.
6. Under **Default Closed Reasons** box, beside **SMS**, select the configured closed reason to apply to SMS message contacts by default.
7. Under **Default Closed Reasons** box, beside **Web Comms**, select the configured closed reason to apply to Web communications contacts by default.
8. Under **Default Closed Reasons** box, beside **Scanned Doc**, select the configured closed reason to apply to scanned documents contacts by default.
9. Under **Default Closed Reasons** box, beside **Voice Mail**, select the configured closed reason to apply to voice mail contacts by default.
10. Click **Save**.

Deleting a closed reason

Before you begin

- Log on to the Contact Center Manager Administration application.

Important:

You can delete only one row at a time.

About this task

Delete a closed reason if you do not want the reason to appear in the Agent Desktop application.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Agent Desktop Configuration**.
3. Click **Resources**.
4. Select a closed reason from the list.
5. Click **Delete**.
6. In the confirmation dialog box, click **Yes**.

Configuring Screen Pops

Before you begin

- Log on to the Contact Center Manager Administration application.
- Use the administration tool on a Contact Center Multimedia server in order to configure intrinsics.

About this task

Use the Screen Pop page to configure application shortcuts and intrinsics. When an agent logs in to Agent Desktop, applications that are configured start automatically.

Important:

Voice Contact Screen Pops are supported only in SIP-enabled contact centers.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Agent Desktop Configuration**.
3. Click **Screen Pop Settings**.
4. Select the **Launch Types** for the configured Screen Pops.
5. Under **Screen Pop Shortcuts**, configure other applications to start on client machines. By default, a text application such as Notepad, or a search engine such as Google can start automatically. You can add other applications, but you must ensure that the applications are installed on all clients. You can configure only one application to force launch.
6. Click **Add** to add more applications.
7. Under **Screen Pop Intrinsics**, configure the intrinsics to display data to the agent. You can configure only one intrinsic to force launch.
8. Click **Add** to add more intrinsics.
9. Click **Contact Screen Pop Intrinsics** to set different intrinsics for the configured contact types. You can select only one intrinsic per contact type.
10. Click **Personal Call Screen Pop Intrinsics** to set the **Inbound** and **Outbound** intrinsics.
11. Select the **Allow Agents select Screen Pop(s)** check box to allow agents to choose the applications they require at the time of launching Agent Desktop.
12. Select the **Launch Screen Pop in a tab inside AAAD** check box to launch Web-based applications inside Agent Desktop. Only Web-based applications launch inside Agent Desktop.

13. Select the **Auto Expand AAAD on Work Item Answer** check box to expand the Agent Desktop application when an agent answers a work item.
14. 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 once an agent releases a contact.
15. Select the desired contact state at which the Screen Pop application is launched from the **Launch State** list.
16. Select the **Launch Screen Pop on Personal Calls** check box to launch Screen Pops during personal calls.
17. Select the **Launch Screen Pop on Outgoing Personal Calls** check box to launch Screen Pops during outbound personal calls.
18. Click **Save**.

Enabling Customer History on Voice Contacts

Before you begin

- Log on to the Contact Center Manager Administration application.
- 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. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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, Advanced Settings page for retrieving the voice history information.

7. Click **Save**.

Configuring Advanced Settings

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

You can specify advanced configuration settings for Agent Desktop.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, 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
Switch Type	The type of PABX that you use in your contact center for voice contacts. Select one of the following: • Sip Avaya Aura 6.1. Select this option when integrating Avaya Aura® Contact

Name	Description
	Center with an Avaya Aura® Unified Communications platform Release 6.1 or 6.2, or an Avaya Aura® Solution for Midsize Enterprise Release 6.1 or 6.2. • CS1K • Sip Avaya Aura 5.2 **Note:** You can select **Sip Avaya Aura 5.2** only if you select **No Switch Configured** while installing Avaya Aura® Contact Center, and you install Contact Center as a multimedia complement to Call Center Elite.
IM Provider	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 • Microsoft OCS, for Microsoft OCS 2007 support • APS, for Avaya Presence Services support **Note:** You can select **APS** only if you select **Sip Avaya Aura 6.1** in the **Switch Type** list.
IM Consult Reporting on Voice Contacts	Enable or disable the reporting of IM 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 real-time 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.

Name	Description
	Note: The default port is 57772, you cannot change this value.
Offsite Agent	Enable Agent Desktop to provide offsite agent capabilities for a CS1K AML Contact Center. **Note:** This field is read-only for all other Contact Center configurations.
Offsite Agent Server	Enter the IP Address or the FQDN of the Avaya Aura® Offsite Agent Server. **Note:** You can enter a value in this field only when the Offsite Agent field is enabled.
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 rate, 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 Observer/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 Phone Book to provide agents with a list of other agents, whom they can consult, during a voice call.

Chapter 50: User configuration

This chapter provides an overview of the User Settings page.

The User Settings page contains configuration settings that you can customize for the Agent Desktop.

Navigation

- User Settings page on page 471

User Settings page

To open the User Settings page, in the CCMM Administration tool, click **Agent Desktop Configuration** and in the left pane click **User Settings**. The User Settings page contains the following fields:

- **Open Queue Contact Processing**—Select **True** 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 Contacts**—Select **True** 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. Customer History on Voice Contacts is supported only in SIP-enabled contact.
- **Display Customer History on Personal Calls**—Select **True** to display customer history for voice contacts on personal calls on Agent Desktop. Customer History on Personal Calls is supported only in SIP-enabled contact.
- **Voice Contact Identifier for Customer History**—Select either AD_CLID or SIP_FROM_ADDRESS to lookup the Contact Center Multimedia database that contains customer history for the originator of the incoming voice call. In order to search the database the ?Voice Contact Search? parameter must be enabled.
- **Encoding Page of CCT Attached Data**—Select 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”
- 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 **True** to suppress browser script errors.

• **Display Not Ready Reason Text Only**—Select **True** to display only not ready reason text.

• **Display Voice Calls in Customer History**—Select **True** 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 here.

• **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 soundcard 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 **True** to ensure an alert is played when voice contacts are presented to agents.
- **Play Alert on CCMM—**Select **True** 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 Agent Desktop's Spark Emulator.

Chapter 51: Data collection and management

The Contact Center Multimedia database contains all multimedia contacts including routing information, customer details, and contact details for e-mail, outbound, instant messages, SMS text message, fax message, scanned documents, voice mail messages, and Web communications. Regular maintenance ensures that the database operates with maximum efficiency. You can periodically archive the information in the database to reduce the data in the multimedia database.

You can archive data in the database by:

- outbound campaign
- e-mail rule
- closed reason
- skillset

Prerequisites for data collection and management

- Determine which type of archive or restore to use.
- Shut down the Multimedia services to prevent issues.

  Important:

  If you modify the data generated from an archive, the data can become corrupt causing future restores to fail. For this reason, Avaya cannot support issues with the application arising from manually modified archive information.
- If your Contact Center Multimedia server is in a domain, you can archive or restore your Contact Center Multimedia database on a network share drive. If your Contact Center Multimedia server is in a workgroup, you cannot use the network drives for the archived data.

Navigation

- Starting the archive utility on page 476
- Archiving by outbound campaign on page 476
- Archiving by e-mail rule on page 477
- Archiving by skillset on page 478
- Archiving by closed reason on page 479
- Restoring an archive on page 480
- Recovering from a failed archive or restore on page 481

Starting the archive utility

Before you begin

- Log on to the Contact Center Multimedia server.

About this task

Start the archive utility to configure your archiving settings and perform the archive or restore of the Contact Center Multimedia database.

Procedure

Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Multimedia Server** > **Archive Restore**.

Archiving by outbound campaign

Before you begin

- Start the archive utility. See Starting the archive utility on page 476.
- Close the Outbound Campaign Management Tool.

About this task

Multiple campaigns can be archived at one time. If you attempt to archive an active campaign, you receive an error message. However, inactive, completed, or cancelled campaigns can be archived.

The Archive utility archives campaign-level information, such as the agent script and associated questions to a file named CampaignArchive.txt, and the all contact data associated with the campaign, such responses to script questions and disposition code data to a file named ContactArchive.txt.

A log file of the archive, ArchiveLogFile.txt, is stored in the archive folder you choose.

Procedure

1. In the archive utility, click the **Archive By Outbound Campaign** tab.
2. From the **Inactive Campaign List**, select the outbound campaign to archive.
3. Click the right arrow to move the selected campaign to the list of campaigns to archive.
4. To include customer data for the contacts in the outbound campaign, clear the **Delete Customer Data** check box.
5. In the **Archive Comments** box, type comments or information about this archive.
6. Under **Archive to Folder**, browse to the folder in which to store the current archive. The folder location you choose for the archive must contain no other files.
7. Click **Archive**.
8. On the calendar, select the date to create your archive.
9. Click **Close**.

Archiving by e-mail rule

Before you begin

- Start the archive utility. See Starting the archive utility on page 476.

About this task

Archive data by e-mail rule. When you archive by e-mail rule, the archive date, by default is six months prior to the current date. When you archive data, you cannot select the current date. Only closed contacts within your selected date range are archived.

Attachment files for e-mail messages are archived in an attachment folder under the folder selected for the archive. All data is archived to a single flat file named ContactArchive.txt. A log file of the archive, ArchiveLogFile.txt, is stored in the archive folder you choose.

The archiving procedure applies to both inline and standard attachments.

Procedure

1. In the archive utility, click the **Archive By Email Rule** tab.

2. Under the **Email Rules List**, navigate through the list of mailboxes and select the rules to archive.
3. Click the right arrow to move the selected rule to the list of items to archive.
4. Repeat step 3 on page 478 for each rule to archive.
5. Under **Contacts Closed on or Before**, click the last date for which you want to archive contacts.
6. To include customer data for the contacts with the selected items, clear the **Delete Customer Data** check box.
7. In the **Archive Comments** box, type comments or information about this archive.
8. Under **Archive to Folder**, type or browse to the folder in which to store the current archive. The folder location you choose for the archive must contain no other files.
9. Click **Archive**.
10. On the Archive Scheduler window, select the start date and time to create your archive.
11. On the calendar, select the date to create your archive.
12. Click **Close**.

Archiving by skillset

Before you begin

- Start the archive utility. See Starting the archive utility on page 476.

About this task

Select a skillset from which to archive data. When you archive by skillset, the archive date, by default six months prior to the selected date. When you archive data, you cannot select the current date. Only closed contacts within your selected date range are archived.

Skillsets that are marked as deleted appear with an asterisk (*).

All contact data is archived to a single flat file named ContactArchive.txt. A log file of the archive, ArchiveLogFile.txt, is stored in the archive folder you choose.

Procedure

1. In the archive utility, click the **Archive By Skillset** tab.
2. Under the **Skillset** list, click a skillset to archive.

   Skillsets in the Skillset list marked with an asterisk are no longer in service.

3. Click the right arrow to move the selected skillset to the list of items to archive.
4. Repeat step 3 on page 479 for each skillset to archive.
5. Under **Contacts Closed on or Before**, click the last date for which you want to archive contacts.
6. To include customer data for the contacts with the selected items, clear the **Delete Customer Data** check box.
7. In the **Archive Comments** box, type comments or information about this archive.
8. Under **Archive to Folder**, type or browse to the folder where you want to store the current archive. The folder location you choose for the archive must contain no other files.
9. Click **Archive**.
10. On the Archive Scheduler window, select the start date and time to create your archive.
11. On the calendar, select the date time to create your archive.
12. Click **Close**.

Archiving by closed reason

Before you begin

- Start the archive utility. See Starting the archive utility on page 476.

About this task

Select a closed reason for which you want to archive data. When you choose to archive by closed reason, the archive date, by default six months prior to the selected date. When you archive data, you cannot select the current date. Only closed contacts within your selected date range are archived.

Closed reasons that are marked as deleted appear with an asterisk (*).

All contact data is archived to a single flat file named ContactArchive.txt. A log file of the archive, ArchiveLogFile.txt, is stored in the archive folder you choose.

Procedure

1. In the archive utility, click the **Archive By Closed Reason** tab.
2. Under the **Closed Reason List**, click a closed reason to archive.

   Closed reasons in the Closed reasons list marked with an asterisk are no longer in service.

3. Click the right arrow to move the selected closed reason to the list of items to archive.
4. Repeat step 3 on page 480 for each closed reason to archive.
5. Under **Contacts Closed on or Before**, click the last date for which you want to archive contacts.
6. To include customer data for the contacts with the selected items, clear the **Delete Customer Data** check box.
7. In the **Archive Comments** box, type comments or information about this archive.
8. Under **Archive to Folder**, type or browse to the folder in which to store the current archive. The folder location you choose for the archive must contain no other files.
9. Click **Archive**.
10. On the Archive Scheduler window, select the start date and time to create your archive.
11. On the calendar, select the date to create your archive.
12. Click **Close**.

Restoring an archive

Before you begin

- Start the archive utility. See Starting the archive utility on page 476.

Important:

If you modify the data generated from an archive, the data can become corrupt causing future restores to fail. For this reason, Avaya cannot support issues with the application arising from manual modification of the data generated by an archive.

About this task

Restore your database from any selected archive. The flat files are added to the database file.

To prepare to restore data, all archived audit records are loaded into the database from the archive location. A progress bar shows the progress of the restore. Do not close the Archive utility during this time. The delay is proportional to the number of archived audit records.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Multimedia Server** > **Archive Restore**.

2. Click **Restore**.
3. In the **Restore** pane, select the archive you want to restore.
4. Click **Restore**.

Recovering from a failed archive or restore

About this task

Restore from a failed archive or restore to recover your archived data. If you experience a problem with the database or Contact Center Multimedia server during an archive or restore, resolve the cause of problem and resume the archiving or restoring to recover your archived data.

Procedure

1. If an archive or restore fails, examine the archive utility **Warnings** box for the cause.
2. Resolve the reported cause.
3. Click **Resume**.

Part VIII: AvayaMediaServer

• configuration configuration on page 485

Chapter 52: Avaya Media Server configuration

This section includes configuration procedures for Avaya Media Server in a SIP-enabled contact center. Avaya Aura® Contact Center uses the media processing capabilities of the Avaya Media Server – Contact Center Services component to support conferencing, announcements, and dialogs in SIP-enabled contact centers.

Prerequisites to Avaya Media Server configuration

- Install Avaya Media Server. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- Install Avaya Media Server. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Logging on to Avaya Media Server Element Manager

Before you begin

• Obtain a valid user name and password to access Avaya Media Server Element Manager.

About this task

Log on to the Avaya Media Server Element Manager as an administrator to configure Avaya Media Server.

Element Manager (EM) is a web-based administration tool that facilitates the Operation, Administration, and Maintenance (OAM) of Avaya Media Server. A SIP-enabled Contact Center solution must contain one or more Avaya Media Server servers. Each Avaya Media Server server in the Contact Center solution must be licensed and configured to provide media services.

Procedure

1. On the Avaya 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 Media Server.

3. In the **User ID** box, type the Avaya Media Server User ID log on account name. The default Element Manager User ID account name is the Avaya MS server administrator account name. If Avaya Media Server is installed on a Windows server, the default administrator account name is *Administrator*. If Avaya Media Server is installed on a Linux server, the default administrator account name is *root*.
4. In the **Password** box, type the Avaya Media Server Element Manager password. The default Element Manager password is the administrator password for the Avaya MS server.
5. Click **Log in**.

Adding the locale-specific media content group

Before you begin

- Create the media content namespace. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

About this task

Using the Avaya Media Server Element Manager, add a locale specific content group to your Content Namespace in the Avaya Media Server Content Store. You use a locale-specific content group to organize your locale-specific custom dialog prompts and music media.

Note:

If your solution has an Avaya Media Server cluster, perform this Content Store procedure only on the primary Avaya Media Server.

Note:

If your solution has a single Avaya Media Server High Availability pair, perform this Content Store procedure only on the primary Avaya Media Server. If your contact center solution has more than one Avaya Media Server High Availability pair, perform this Content Store procedure only on the Avaya Media Server High Availability Content Store master pair. Avaya Media Server High Availability Content Store replication duplicates this Content Namespace to all other Avaya Media Servers in your solution.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **Tools** > **Media Management**.
3. On the **Media Management** page, under **Content Namespaces**, select the content namespace.

4. Click **Browse**.
   Avaya MS displays the Provision Media page.
5. On the **Provision Media** page, in the left pane, select the content namespace.
6. Click **Add Content Group**.
   Avaya MS displays the New Content Group page.
7. In the **New Content Group** dialog box, in the **Name** box, type the name for the locale-specific content group.

   Important:

   This content group must match the Local SIP Subscriber MS Locale in Contact Center Manager Server–Server Configuration.
8. Click **Save**.

Uploading a batch zip file

Before you begin

- Add the content namespace. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).
- 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 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.

To provision a single media file, see Uploading a treatment media file on page 491.

Note:

If your solution has an Avaya Media Server cluster, perform this Content Store procedure only on the primary Avaya Media Server.

Note:

If your solution has a single Avaya Media Server High Availability pair, perform this Content Store procedure only on the primary Avaya Media Server. If your contact center solution has more than one Avaya Media Server High Availability pair, perform this Content Store procedure only on the Avaya Media Server High Availability Content Store master pair. Avaya Media Server High Availability Content Store replication duplicates this Content Namespace to all other Avaya 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 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**.

Adding a media content group

Before you begin

- Create the media content namespace. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

About this task

Add a content group to contain music media. You can add multiple media content groups to a content namespace. A music content group typically contains music of one category, for example instrumental or jazz music. Contact Center uses music media to provide scripted music in Contact Center Orchestration Designer (OD) flow applications or scripts.

Note:

Skip this procedure if Avaya Media Server uses a continuous streamed music source.

Note:

If your solution has an Avaya Media Server cluster, perform this Content Store procedure only on the primary Avaya Media Server.

Note:

If your solution has a single Avaya Media Server High Availability pair, perform this Content Store procedure only on the primary Avaya Media Server. If your contact center solution has more than one Avaya Media Server High Availability pair, perform this Content Store procedure only on the Avaya Media Server High Availability Content Store master pair. Avaya Media Server High Availability Content Store replication duplicates this Content Namespace to all other Avaya Media Servers in your solution.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **Tools** > **Media Management**.
3. On the **Media Management** page, under **Content Namespaces**, select the content namespace.
4. Click **Browse**.
   Avaya MS displays the Provision Media page.
5. On the **Provision Media** page, in the left pane, select the content namespace.
6. Click **Add Content Group**.
   Avaya MS displays the New Content Group page.
7. In the **New Content Group** dialog box, in the **Name** box, type a name for the new content group.
8. Click **Save**.

Uploading a music media file

Before you begin

- Upload the music .WAV file, encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec, to a folder on the Avaya MS server.
- Add a content namespace. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).
- Add a content group. For more information about adding a content group, see Adding a media content group on page 488.

About this task

Upload a music file to provision music for the Avaya Media Server. The music file is used to provide scripted music from an Orchestration Designer (OD) flow application or script.

To be able to use the music in an OD flow application or script, you must configure and acquire a route for the content group using the Configuration page of CCMA. This route name must match the content group described in the steps below. For more information, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

To provide music to callers, add or edit a flow application or script to provide scripted music using OD, using the Route Number entered in the Configuration page of CCMA. For more information, see *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (NN44400-510).

Note:

Skip this procedure if Avaya Media Server uses a continuous streamed music source.

Note:

If your solution has an Avaya Media Server cluster, perform this Content Store procedure only on the primary Avaya Media Server.

Note:

If your solution has a single Avaya Media Server High Availability pair, perform this Content Store procedure only on the primary Avaya Media Server. If your contact center solution has more than one Avaya Media Server High Availability pair, perform this Content Store procedure only on the Avaya Media Server High Availability Content Store master pair. Avaya Media Server High Availability Content Store replication duplicates this Content Namespace to all other Avaya Media Servers in your solution.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **Tools** > **Media Management**.

3. On the **Media Management** page, select the check box next to the content namespace.
4. Click **Browse**.
   Avaya MS displays the Provision Media page.
5. On the **Provision Media** page, expand the content namespace.
6. Select the content group to which you want to add a music file.
7. Click **Add Media**.
   Avaya MS displays the Add Media dialog.
8. In the **Add Media** dialog box, click **Browse** and navigate to the music file on the server.
9. Click **Upload**.

Uploading a treatment media file

Before you begin

- Upload the treatment .WAV file, encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec, to a folder on the Avaya MS server.
- Add the content namespace. For more information, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).
- Add the locale-specific content group. For more information about adding a content group, see Adding the locale-specific media content group on page 486.

About this task

Using Avaya Media Server Element Manager, upload a media file to provide call treatments, such as announcements. Treatment media files must be stored in the locale-specific content group that matches the locale of the contact center.

To be able to use the treatment in an OD flow application or script, you must configure and acquire a route for the treatment file using the Configuration page of CCMA. This route name must exactly match the treatment file described in the steps below. For more information, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

To provide treatments to callers, add or edit a flow application or script to provide treatments using OD, using the Route Number entered in the Configuration page of CCMA. For more information, see *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (NN44400-510).

Note:

Skip this procedure if Avaya Media Server uses a continuous streamed music source.

Note:

If your solution has an Avaya Media Server cluster, perform this Content Store procedure only on the primary Avaya Media Server.

Note:

If your solution has a single Avaya Media Server High Availability pair, perform this Content Store procedure only on the primary Avaya Media Server. If your contact center solution has more than one Avaya Media Server High Availability pair, perform this Content Store procedure only on the Avaya Media Server High Availability Content Store master pair. Avaya Media Server High Availability Content Store replication duplicates this Content Namespace to all other Avaya Media Servers in your solution.

Procedure

1. Log on to Element Manager.
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 treatment media.
4. Click **Browse**.
   Avaya MS displays the Provision Media page.
5. On the **Provision Media** page, expand the content namespace.
6. Select the locale-specific content group.
7. Click **Add Media**.
   Avaya MS displays the Add Media dialog.
8. In the **Add Media** dialog box, click **Browse** and navigate to the media file on the server.
9. Click **Upload**.

Part IX: Managing Security

- Security Fundamentals on page 495
- Platform Security on page 499
- Security Template on page 503

Chapter 53: Security Fundamentals

Secure Avaya Aura® Contact Center to enable the user to secure the different applications available.

Navigation

- Simple Network Management Protocol on page 495
- Event viewer settings on page 495
- Event Browser and Alarm Monitor on page 496
- Logon warning message (CCMA and UCM) on page 497
- Systems Management Server security file (Multimedia) on page 497
- Contact Center Manager Server Utility to view events on CCMS on page 498

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. For more information about the features, see Event Browser versus Alarm Monitor features on page 106.

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.

Logon warning message (CCMA and UCM)

The logon message is the standard message used by Microsoft Windows. This is the same Microsoft Windows message that appears when you log on to Microsoft Windows.

In CCMA, you can configure the message title and text of the warning message if you do not have a domain security policy in place with a logon warning message configured.

UCM also provides the text for the logon warning message that a security administrator can change. For more information, see *Avaya Unified Communications Management Common Services Fundamentals (NN43001-116)*.

Systems Management Server security file (Multimedia)

The Systems Management Server (SMS) also known as the Avaya Multimedia security policy file, CCMM_Security_Policy.msi (Microsoft Installer), contains a policy level for the client to download and run assemblies with a particular strong name. A strong name consists of the assembly identity (name, version number, private key) and a public key. The Outbound Campaign Management Tool and the Agent Desktop assemblies are digitally signed with a strong name based on the private key. After it is installed, the CCMM_Security_Policy.msi file instructs the clients to trust the assemblies with the strong name assigned to the Outbound campaign Management Tool and the Agent Desktop. You can install the CCMM_Security_Policy.msi file while you are logged on to the server as the local administrator.

To install the security policy, you must install the current Avaya CCMM_Security_Policy.msi file that is included in the most recent service pack. Avaya recommends the SMS to install the msi file on multiple clients.

Because installation procedures through an SMS system can vary from one company to the next, follow your company guidelines to install the CCMM_Security_Policy.msi file for the SMS clients on your network. For more information, see the SMS documentation on the Microsoft Web site at www.microsoft.com.

Experienced system administrators can deploy the CCMM_Security_Policy.msi file.

Group policy

In addition to using an SMS server, a system administrator can install the CCMM_Security_Policy.msi file on clients within the same domain using a Windows group policy. For details, see document 324750 on the Microsoft knowledge base.

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 54: Platform Security

Windows allows you to configure security features that help you secure your server. The Security Configuration Wizard is part of Windows Server 2008 Release 2.

Navigation

- Securing the Server on page 499

Securing the Server

Before you begin

- Ensure the Contact Center application server is running.

About this task

Select minimum options when running the Security Configuration Wizard on your Contact Center application server. You can create a less restrictive policy by enabling other services and server roles depending on your requirements.

Procedure

1. On the **Start** menu, click **Run**.
2. Type SCW, and then click **OK**.
3. In the Welcome window, click **Next**.
4. In the Configuration window, select **Create a New Security Policy**, and then click **Next**.
5. Ensure the host name of the local server is correct, and then click **Next**.
6. After the processing of the security configuration database is finished, click **Next**.
7. In Role-Based Service Configuration window, click **Next**.
8. In the Select Server Roles window, select the **Web Server** check box, and then click **Next**.

Important:

Some of the following steps require specific selections according to your application. If this occurs, contact your administrator.

9. In the Select Client Features window, select the client features you want to enable according to your application server.

   As a minimum, Avaya recommends that you select the features already enabled according to the specified application server.

10. Click **Next**.
11. On the **Select Administration and Other Options** dialog box, select the server features that you want to enable.

    As a minimum, Avaya recommends that you select the features already enabled according to the specified application server.

12. Click **Next**.
13. Select the services you want to enable.

    You must enable the required services for each Contact Center application server to function correctly.

    Select services that you require such as antivirus software clients.

14. Click **Next**.
15. In the **Handling Unspecified Services** dialog box, select one the following options:

If	Then
You want to disable all services on the server that are not defined in the security policy.	Select **Disable the service**.
You want to avoid changing the startup mode of the services on the server that are not defined in the security policy.	Select **Do not change the startup mode of the service**.

16. Click **Next**.
17. In the Confirm Service Changes window, review the modified services when you apply this policy to your system.
18. Click **Next**.
19. In the Network Security window, click **Next**.
20. In the Network Security Rules window, select the rules that you want to view from the **View** drop-down list.
21. Select the roles and administrative options that require Firewall rules.

22. Optional: To edit a rule, select the rule in the Network Security Rules window.
23. Optional: Click **Edit** and then select the options that apply to your server.
24. Optional: Click **OK**.
25. Click **Next**.
26. In the Registry Settings window, click **Next**.
27. In the Require SMB Security Signatures window, select the **All computers that connect to it satisfy the following minimum operating system requirements** check box.
28. Clear the **It has surplus processor capacity that can be used to sign file and print traffic** check box, and then click **Next**.
29. In the Outbound Authentication Methods window, select only the **Domain Accounts** box. Ensure that you clear the other check boxes, and then click **Next**.
30. In the Outbound Authentication using Domain Accounts window, select the **Windows NT 4.0 Service Pack 6a or later systems** check box.
31. Clear the **Clocks that are synchronized with the selected server's clock** check box, and click **Next**.
32. Review the Registry Settings Summary, and then click **Next**.
33. In the Audit Policy window, click **Next**.
34. In the System Audit Policy window, select your auditing objective. The available options are **Do not audit**, **Audit successful activities**, and **Audit successful and unsuccessful activities**.
35. Click **Next**.
36. Review the **Audit Policy Summary**, and then click **Next**.
37. In the Save Security Policy window click **Next**.
38. In the Security Policy File Name window, click **Browse**, and browse to select the location in which to save the security policy file.
39. In the **Save As** dialog box, type the file name for the security policy file.
40. In the Apply Security Policy window, select whether you want to apply the security policy to the selected server now or later. The options are **Apply now** or **Apply later**.
41. Click **Finish**.

Chapter 55: Security Template

Contact Center provides a set of predefined Windows Server 2008 Release 2 Security Templates that you can deploy quickly to secure the Contact Center suite of servers.

The following procedures allow you to activate and apply these templates.

Navigation

- Activating the Contact Center security template on page 503
- Applying the security template locally on the server on page 504
- Applying the security template in a network domain on page 506

Activating the Contact Center security template

About this task

You can activate the Contact Center security template locally or as a group policy in an Active Directory that contains the Contact Center suite of application servers. You can deploy the Security Template either before or after you install the server software.

If you activate the Contact Center Security Template locally (on the server on which you installed Contact Center Multimedia/Outbound), you must select the applicable Security Template for the Contact Center application server and download the selected template from the Enterprise Solution PEP Library web site (www.avaya.com/support) to the local disk drive. After you download the file, you can import and configure the Security Template using the Microsoft Security Configuration and Analysis utility.

If you want to activate the Avaya Contact Security Template on a coresident server, make sure that you download the coresident template.

If you are adding the Communication Control Toolkit to a previously stand-alone Contact Center Manager Server, you must rollback the original Contact Center security template and reapply a new one for the coresident server.

Procedure

1. Log on to the server as Administrator.
2. In the Windows **Start** menu, click **Run**.

3. Type `mmc`, and then click **OK**.
4. In the Console1 window, from the **File** menu, choose **Add/Remove Snap-in**.
5. On the **Add/Remove Snapin** dialog box, click **Add**.
6. Select **Security Configuration and Analysis,** and then click **Add**.
7. Click **OK**.
8. On the console, right-click **Security Configuration and Analysis.**
9. Click **Open Database**.
10. In the **File Name** box, enter a new database name. For example, type `CCM_Outbound_Security`.
11. Click **Open**.
12. Select **Contact Center Multimedia/Outbound Security Template.inf**, and then click **Open**.
13. On the console, right-click **Security Configuration and Analysis**, and then click **Analyze Computer Now**.

    The **Perform Analysis** dialog box appears. The default location for the Security Template log is C:\Documents and Settings\Administrator\My Documents\Security \Logs\. If you want to change the location in which the Security Template log is stored, do so now.
14. Click **OK**.
15. Right-click **Security Configuration and Analysis**, and then choose **Configure Computer Now**.

    The **Configure System** dialog box appears. The default location for the configuration log file is C:\Documents and Settings\Administrator\My Documents \Security\Logs\. If you want to change the location in which the Security Template log is stored, do so now.
16. Click **OK**.
17. Restart the server to activate the new security policy and configuration.

Applying the security template locally on the server

About this task

You can activate the Contact Center security template locally or as a group policy in an Active Directory that contains the Contact Center suite of application servers. You can deploy the security template either before or after you install the server software.

If you activate the Contact Center security template locally (on the server on which you installed Contact Center Multimedia/Outbound), you must select the applicable Security Template for

the Contact Center application server and download the selected template from the Enterprise Solution PEP Library web site (www.avaya.com/support) to the local disk drive. After you download the file, you can import and configure the Security Template using the Microsoft Security Configuration and Analysis utility.

Procedure

1. Log on to the server as Administrator.
2. In the Windows **Start** menu, click **Run**.
3. Type `mmc`, and then click **OK**.
4. In the Console1 window, from the **File** menu, choose **Add/Remove Snap-in**.
5. On the **Add/Remove Snapin** dialog box, click **Add**.
6. Select **Security Configuration and Analysis**, and then click **Add**.
7. Click **OK**.
8. On the console, right-click **Security Configuration and Analysis.**
9. Click **Open Database**.
10. In the **File Name** box, enter a new database name. For example, type `Contact Center Multimedia/Outbound Security Template`.
11. Click **Open**.
12. Select **Contact Center Multimedia/Outbound Security Template.inf**, and then click **Open**.
13. On the console, right-click **Security Configuration and Analysis**, and then click **Analyze Computer Now**.

    The **Perform Analysis** dialog box appears. The default location for the Security Template log is C:\Documents and Settings\Administrator\My Documents\Security \Logs\. If you want to change the location in which the Security Template log is stored, do so now.
14. Click **OK**.
15. Right-click **Security Configuration and Analysis**, and then choose **Configure Computer Now**.

    The **Configure System** dialog box appears. The default location for the configuration log file is C:\Documents and Settings\Administrator\My Documents \Security\Logs\. If you want to change the location in which the Security Template log is stored, do so now.
16. Click **OK**.
17. Restart the server to activate the new security policy and configuration.

Applying the security template in a network domain

Before you begin

- Download Group Policy Management Console (GPMC) from microsoft.com, and install it on the server.

About this task

Apply the Contact Center security templates in a network domain environment by importing the template into a group policy object of an organizational unit (OU) of which the Contact Center server is a member.

Procedure

1. Open **GPMC**.
2. In the console tree, expand the domain or OU that you want to import to the Security Template.
3. Right-click the Group Policy object you want to edit, and then click **Edit**.
4. On the **Group Policy Object Editor** console tree, click **Computer Configuration**.
5. Click **Windows Settings**, and then right-click **Security Settings**.
6. Click **Import Policy**.
7. Select the Security Template that you want to import, and then click **Open**.

Part X: Common server administration

- Microsoft Windows configuration and management on page 509
- Simple Network Management Protocol administration on page 515
- Licensing administration on page 519
- Contact Center database maintenance on page 525
- Contact Center server High Availability on page 537
- Common procedures on page 559

Chapter 56: Microsoft Windows configuration and management

Perform the following procedures to configure settings in Microsoft Windows on your servers.

Navigation

- Managing date and time features on page 509
- Disabling the Windows time service on page 510
- Verifying Service Packs on page 511
- Configuring the operating system for remote access in a domain on page 511
- Configuring the operating system for remote access in a workgroup on page 512

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. Click **Start** > **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 the **Internet Time** tab.

   Important:

   If you click this tab and click OK without making changes, the Startup type for the Windows Time service is Automatic.

9. Click **Change settings**.
10. Clear the **Synchronize with an Internet time server** check box.
11. Click **OK** to save your changes.
12. Click **OK**.

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 aSIP environment or is the Network Control Center server, you must skip this step.

Procedure

1. Click **Start** > **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 *Avaya Aura® Contact Center Upgrade and Patches* (NN44400-410) 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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **Contact Center Patch Manager**.
3. Click the **Manager Server** tab.
4. View the most recent **Update Name**.
5. Compare the most recent update name in the Patch Manager with the most recent patch or upgrade listed on the Avaya Web site.
6. Click **Close**.
7. Install missing Service Packs from the Web site by performing instructions present in *Avaya Aura® Contact Center Upgrade and Patches* (NN44400-410).

Configuring the operating system for remote access in a domain

Before you begin

- Add your server to the domain.

About this task

Configure remote access for your server in a domain to allow technical support to access the server.

Procedure

1. Log on to the server.
2. Click **Start** > **All Programs** > **Administrative Tools** > **Routing and Remote Access**.
3. Right-click the local server name, and then select **Configure and Enable Routing and Remote Access**.
4. Click **Next**.
5. Select **Remote Access (dial-up or VPN)**.
6. Click **Next**.
7. Click **Dial-up**.
8. Click **Next**.
9. Select the network connection that represents your contact center subnet.
10. Click **Next**.
11. Select **From a specified range of addresses**.
12. Click **Next**.
13. Click **New**.
14. Enter the range of IP addresses provided by your domain administrator.
15. Click **OK**.
16. Click **Next**.
17. Select **No, use Routing and Remote Access to authenticate requests**.
18. Click **Next**.
19. Click **Finish**.

Configuring the operating system for remote access in a workgroup

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. Click **Start** > **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 57: Simple Network Management Protocol administration

Windows provides a Simple Network Management Protocol (SNMP) agent, which runs as a service on each Avaya Aura® Contact Center server. Avaya Aura® Contact Center servers use this service to forward events to a Network Management System (NMS) on your network.

Caché database automatically forwards SNMP traps for important database events. As long as the SNMP feature is added to the server before installation then once the Windows SNMP is configured to forward events to the NMS, no further user intervention is required to enable the SNMP traps for Caché. The Caché database events are applicable to the Avaya Aura® Contact Center servers with Caché database installed (Contact Center Manager Server, Communication Control Toolkit, and Contact Center Multimedia).

For more information about event codes and a list of recommended events to forward, see *Avaya Aura® Contact Center Contact Center Event Codes* (NN44400-713).

This chapter describes how to configure the Simple Network Management Protocol for your contact center.

Navigation

- Installing Windows SNMP Service on page 515
- Selecting CCMS events to be forwarded on page 516
- Selecting CCMA, CCT, and CCMM events to be forwarded on page 517
- Configuring the NMS on page 518

Installing Windows SNMP Service

About this task

Install Windows Simple Network Management Protocol (SNMP) agent on each Avaya Aura® Contact Center server to forward events to a Network Management System (NMS) on your network.

Procedure

1. Log on to the server as Administrator.
2. Click **Start** > **All Programs** > **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. From the **Start** menu, choose **All Programs** > **Accessories** > **Windows Explorer**.
2. Browse to the folder **D:\Avaya\Contact Center\Manager Server\bin**, and double-click **SNMPFilterCnfg.exe**.
3. 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.

4. Click **OK**.

Selecting CCMA, CCT, and CCMM events to be forwarded

About this task

Contact Center Manager Administration, Communication Control Toolkit, and Contact Center Multimedia use the Windows Server 2008 Event to Trap Translator (evntwin.exe) to select the events to be forwarded to the Network Management System (NMS).

For more information about event codes and a list of recommended events to forward, see *Avaya Aura® Contact Center Contact Center Event Codes* (NN44400-713).

Procedure

1. Click **Start** > **Run**.
2. In the **Run** text box, type `C:\Windows\System32\evntwin.exe`
3. Click **OK**.
4. On the **Event to Trap Translator**, under **Configuration type**, select **Custom**.
5. Click **Edit**.
6. 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.
7. From the list of events, double-click the event source you want to convert to an SNMP trap.
8. On the Properties window, click **OK** if no change is required to generate the trap.
9. Repeat step 7 on page 517 and step 8 on page 517 for each event that you want added to the list of events to be translated into SNMP traps.

   Important:

   For a list of recommended events to forward to the Network Management System, see *Avaya Aura® Contact Center Contact Center Event Codes* (NN44400-713).

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 Avaya Aura® 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:

- nt-ref.mib (MIB-II)
- nbflt.mib (NGen MIB)
- RR-Nortel.mib (Resiliency MIHB)

You can use these files on the NMS system. They are SNMP v1 MIB files. The nt-ref.mib and nbflt.mib files are available in Contact Center Manager Server, in the D:\Avaya\data, and RR-Nortel.mib can be found in <InstallDirectory>\Avaya\Contact Center\Common Components \Cache.

Procedure

For more information about configuring your NMS, see your NMS documentation.

Chapter 58: 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.

Important:

Avaya Media Server does not support the grace period. When Avaya Media Server is co-resident with Contact Center License Manager, if the licensing services stop, Avaya Media Server stops and Contact Center ceases processing voice contacts. For more information about the licensing requirements for Avaya Media Server, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

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

Navigation

- Resetting the grace period on page 520
- Updating the license file on page 521
- Changing from Nodal to Corporate licensing on page 521
- Changing the licensing information on Contact Center Manager Server on page 523
- Refreshing your server on page 524

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 520 to step 6 on page 520.
- 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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **Grace Period Reset** to apply the new unlock code.
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 Utility.

Procedure

1. Log on to the server where the Contact Center License Manager software is installed.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **License Manager** > **Configuration**.
3. On the Configuration page, click **Browse**.
4. View the type of license file currently used, and then click **OK**.
5. Navigate the file system and locate the new license file.
6. Click **Open**.
7. Click **Apply**.
8. If you are using a WebLM license file or if you are changing from PLIC to WebLM licensing, then on the Contact Center License Manager server, restart the Contact Center Tomcat Instance service.
9. At the prompt, click **Yes** to restart the Contact Center License Manager server.
10. Click **OK** to close the window.
11. Click **Exit**.

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 **Start** menu, click **All Programs** > **Avaya** > **Contact Center** > **License Manager** > **Configuration**.
3. On the Configuration page, click **Browse**.
4. Navigate the file system and locate the new license file.
5. Click **Open**.
6. Click **Apply**.
7. Click **Yes** to restart the Contact Center License Manager Server service.
8. Click **OK** 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 on page 523.
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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **License Manager** > **Configuration**.
14. On the Configuration page, click **Browse**.
15. Navigate the file system and locate the new license file.
16. Click **Open**.
17. Click **Apply**.
18. Click **Yes** to restart the Contact Center License Manager Server service.
19. Click **Exit** to close the window.

20. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
    The Initializing Server Configuration Utility window appears. This window can remain open for up to 30 seconds.
21. If you have a co-resident Contact Center License Manager, an information box may appear. If it does, click **Continue**.
22. Click **Licensing**.
23. Under **License Manager Package**, change the package to the corporate version.
24. Under **License Server IP Address**, type the correct IP information for the Primary and Secondary Contact Center License Manager IP address.
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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **License Manager** > **Shutdown**.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
3. Click **Licensing**.
4. Under **License Manager Package**, change the **CCMS Package** and **Optional Packages** information to reflect your new licensed options.
5. Under **License Server IP Address**, type the correct IP information for the Primary and Secondary Contact Center License Manager IP address.
6. Click **Apply All**.

7. 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.
2. On the launchpad, click **Configuration**.
3. On the **Server** menu, click **Refresh All Servers**.
4. Click **Yes**.

Chapter 59: Contact Center database maintenance

Contact Center Manager Server, Communication Control Toolkit and Contact Center Multimedia each have their own Caché database. They use a common database backup and restore utility. Perform the procedures in this chapter to back up or restore one or more Contact Center database.

Contact Center Manager Server has an Integrated Reporting (IR) capability for Multimedia (CCMM) and Avaya Media Server statistics. To access Avaya Media Server-Contact and Multimedia-Contact summary reports configure Integrated Reporting using the Database Maintenance utility.

Contact Center Manager Server, Communication Control Toolkit (CCT) and Contact Center Multimedia (CCMM) each have their own Caché database. CCT and CCMM may be installed co-resident with CCMS. The CCT, CCMS, and CCMM databases must be backed-up at the same time and stored as a matching or synchronized set. They must also be restored together to ensure the restored systems have synchronized configuration and statistical data.

Prerequisites to Contact Center server database maintenance

- Ensure that the Contact Center software is installed.

Navigation

- Creating a backup location on page 526
- Performing an immediate backup of the database on page 527
- Scheduling a backup of the database on page 529
- Recovering a scheduled backup on page 531
- Restoring a backup on page 531
- Migrating the database on page 533
- Configuring Integrated Reporting on page 534

Creating a backup location

Before you begin

- Ensure that you have a user account with full read and write permissions to the location for the database backups.

About this task

Create a backup location with the correct access permissions on your network.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
2. In the **Database Maintenance** dialog box, in the left pane, expand **Backups**.
3. Click **Backup Locations**.
4. In the right pane, click **Create**.
5. From the **Drive Letter** list, select a drive letter.
6. In the **UNC Path** text box, type the location to which to backup the database.
7. In the **Username** box, type the user name used to log on to the server specified in the UNC Path box.
8. In the **Password** box, type the domain password.
9. Click **OK**.

Variable definitions

Name	Description
Drive Letter	The drive letter representing the destination for the backup file. You can choose from the drive letters listed.
UNC Path	The Uniform Naming Convention (UNC) path, which is the IP Address and folder name of the server destination for the backup file. For example, the UNC path can be \ \192.167.140.0\backup.

Name	Description
Username	The user name, including server name and user name for the backup destination server. For example, the user name can be 192.167.140.45\administrator.
Password	The password for the user that you configure for the backup location.

Performing an immediate backup of the database

Before you begin

- Create a backup location if you want to use a network location for your backup.
- Know which applications you are to back up.

Important:

The CCT, CCMS, and CCMM databases must be backed-up at the same time and stored as a matching or synchronized set. They must also be restored together to ensure the restored systems have synchronized configuration data.

About this task

Perform an immediate backup of the database to save the current data. You must perform this procedure after installation or when any significant change occurs in the database, so that you can easily restore the database.

You can back up one or more Contact Center databases at one time. The backup folder contains separate backup files for each database or folder you select.

CCMS Services are not shut down during backups, however create backups during low traffic periods.

If your contact center is running with a standby server, ensure that you back up the primary server, not the standby server.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
2. In the **Database Maintenance** dialog box, in the left pane, click **Immediate Backup**.
3. In the **Media Type** section, select the **Tape Drive** or **Network Disk** option.
4. In the **Applications** section, select the check box beside each application to back up.

5. From the **Backup Location** list, select the network drive where you want to store the backup.
6. Click **Backup**.
7. Click **Yes** to confirm your choices.
8. Use the **Progress information** field to monitor the progress of the backup.
9. Click **Exit** to close the Database Maintenance utility.

Variable definitions

Name	Description
Applications	The Contact Center application databases that you can back up: • CCMS: Contact Center Manager Server database • CCT: Communication Control Toolkit database • CCMM: Contact Center Multimedia database • ADMIN: Configuration items for backup locations, redundancy paths and schedule information (not an application database) If an application is not available, you cannot select it.
Backup Location	The destination for the network disk. The values are configured in the Backup Locations.
Media type	The type of media used for your backup file. You can use a network disk location or a tape drive. If you use a network disk location, you must configure a destination before you can back up the file.

Scheduling a backup of the database

Before you begin

- Create a backup location.
- Know which applications you are to back up.

Important:

The CCT, CCMS, and CCMM databases must be backed-up at the same time and stored as a matching or synchronized set. They must also be restored together to ensure the restored systems have synchronized configuration data.

About this task

Schedule a backup of the Contact Center server database to save the data regularly. You must regularly back up the database to ensure you always have current information in case you need to restore the data.

Regularly scheduled backups overwrite the same file each time they occur. To keep more than one backup file, you must configure a separate network drive.

You can back up one or more databases at one time. The backup folder contains separate backup files for each database or folder you select. If you have two scheduled backups occurring at the same time, the backup with the longer timeframe occurs first. For example, if you have a weekly backup and a monthly backup scheduled at the same time, the monthly backup runs first.

If your contact center is running with a standby server, ensure that you back up the primary server, not the standby server, to back up the most current data.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
2. In the **Database Maintenance** dialog box, in the left pane, click **Scheduled Backup**.
3. In the right pane, click **Create**.
4. Under **General Properties**, in the **Name** box, type a name for the scheduled backup.
5. From the **Media Type** list, select **Network Location**.
6. In the **Start Date** box, type the date on which to begin scheduled backups.

   OR

   Click the calendar icon and select a date on which to begin scheduled backups.
7. In the **Start Time** box, select the time to start the backup.

8. From the **Backup Location** list, select a drive to store the backup.
9. From the **Frequency** list, select the frequency of the backup.
10. Under **Applications**, select the check box beside the applications to back up.
11. Click **OK**.
12. Click **Exit** to close the Database Maintenance utility.

Variable definitions

Name	Description
Applications	The Contact Center application databases that you can back up: • CCMS: Contact Center Manager Server database • CCT: Communication Control Toolkit database • CCMM: Contact Center Multimedia database • ADMIN: Configuration items for backup locations, redundancy paths and schedule information (not an application database) If an application is not available, you cannot select it.
Backup Location	The destination for the network disk. The values are configured in the Backup Locations.
Frequency	The frequency of the backup. You can choose from daily, weekly, monthly, or run once.
Media type	The type of media used for your backup file. You can use a network disk location or a tape drive. If you use a network disk location, you must configure a destination before you can back up the file.
Name	Identifier for the scheduled backup. You can identify each backup with a unique name.

Recovering a scheduled backup

Before you begin

- Ensure that you view the event in Windows Event Viewer and address the reason why the scheduled backup failed.

About this task

Recover a scheduled backup if an error occurs while the backup is running. A scheduled backup failure can occur for several reasons. For example, if the backup location is not available or if there is not enough space to save the backup file, the scheduled back up fails. If an error occurs, the scheduled backup stops and an event is created. View the event in the Windows Event Viewer.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
2. In the **Database Maintenance** dialog box, in the left pane, click **Scheduled Backup**.
3. Click the name of the scheduled backup to recover.
4. Click **Recover**.
5. Click **OK**.

Restoring a backup

Before you begin

- Ensure that you know the location of the backup file.
- Ensure that you know which database to restore.

Important:

The CCT, CCMS, and CCMM databases must be backed-up at the same time and stored as a matching or synchronized set. They must also be restored together to ensure the restored systems have synchronized configuration data.

About this task

Restore a backup of one database at a time to your servers to restore the database to the point at which the last backup occurred if you encounter a database error.

If you have a co-resident server, restore the databases in the order that the software was installed, Contact Center Manager Server, Communication Control Toolkit second, then Contact Center Multimedia database, then administration files.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
2. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
3. In the right pane, under **Media Type**, select the media type on which the backup is restored.
4. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
5. Under **Application**, select the database (CCT, CCMS, or CCMM) or administration (ADMIN) files to restore.
6. Under **Restore contents**, choose the contents to restore for the database.
7. Click **Restore**.
8. Use the **Progress information** field to monitor the progress of the restore.
9. Click **Exit** to close the Database Maintenance utility.

Variable definitions

Name	Description
Application	The database and applications of Contact Center that you can back up: • CCT: Communication Control Toolkit database • CCMS: Contact Center Manager Server database • CCMM: Contact Center Multimedia database • ADMIN: Configuration items for backup locations, redundancy paths and schedule information (not an application database)
Backup Location	The destination for the network disk. The values are configured in the Backup Locations.

Name	Description
Restore contents	The type of content stored in the database. Data is the data in the database or application file. Schema is the information for Web services on the Contact Center Multimedia database.
Media type	The type of media used for your backup file. You can use a network disk location or a tape drive. If you use a network disk location, you must configure a destination before you can back up the file.

Procedure job aid

When you restore a Contact Center Multimedia database, if you restore the database backup to a Multimedia server different from where the backup occurred, the e-mail attachments are restored to the original installation attachments folder (\Avaya\Contact Center\Email Attachments\).

After the restore, you must confirm that the E-mail Configuration settings in the CCMM administrator point to the correct attachments folder.

Migrating the database

Before you begin

- Ensure that your database from the previous release of Contact Center is converted to the Caché format. For more information, see *Avaya Aura® Contact Center Upgrade and Patches* (NN44400-410).
- Back up the old database.
- Know the drive on your server on which your database is installed.
- Create a backup location. See Creating a backup location on page 526.

About this task

Migrate the database from one server to another. You can also migrate a database from a previous release to the current release.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
2. In the **Database Maintenance** dialog box, in the left pane, click **Migration**.
3. In the right pane, select the **Application** from which you want to migrate.
4. In the **Migration Location** box, select the location for your current database backup.
5. Click **OK**.

Variable definitions

Name	Description
Application	The possible applications from where you can select a database. For example, if you are on a Contact Center Manager Server, you can migrate a database from a previous release.
Migration Location	The location on the network for the database backup.

Procedure job aid

When you migrate a Contact Center Multimedia database, if you restore the database backup to a new Multimedia server, the e-mail attachments are restored to the original installation attachments folder (\Avaya\Contact Center\Email Attachments\).

After the restore, you must confirm that the E-mail Configuration settings in the CCMM administrator point to the correct attachments folder.

Configuring Integrated Reporting

About this task

To access Avaya Media Server-Contact Summary reports and Multimedia-Contact Summary reports, configure Integrated Reporting in Database Maintenance utility.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
2. in the Database Maintenance window, in the left panel, click **Integrated Reporting Server**.
3. In the right panel, click **Create**.
4. From the **Type list**, select **ICP**.
5. In the **Display Name** box, type the server name.
6. In the **Username** box, type the username to log on to the server in the name box.
7. In the **Password** box, type the domain password.
8. Click **OK**.
9. In the right panel, click **Create**.
10. From the type list, select **Multimedia**.
11. Repeat step 5 on page 535 to step 8 on page 535.
12. To close the **Database Maintenance** utility, click **Exit**.

Variable definitions

Name	Description
server name	The display name that depends on the server type: Avaya Media Server or Multimedia.

Chapter 60: 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
- Warm standby High Availability

Mission Critical High Availability:

Avaya Aura® Contact Center supports Mission Critical High Availability for a pair of co-resident Contact Center Manager Server (CCMS) and Communication Control Toolkit (CCT) servers in a campus environment with the following:

- SIP-enabled contact center with an Avaya Aura® Communication Manager and an Avaya Aura® Session Manager Release 6.1 or later.

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 Media Server, CCMA, and CCMM services does not affect the available SMMC system tray menu options.

Hot-standby High Availability:

Avaya Aura® Contact Center supports hot-standby High Availability for a pair of co-resident Contact Center Manager Server (CCMS) and Communication Control Toolkit (CCT) servers in a campus environment with the following:

- AML-based contact center with an Avaya Communication Server 1000 PABX.

Warm standby High Availability:

Avaya Aura® Contact Center supports warm standby High Availability for a pair of co-resident Contact Center Manager Server (CCMS) and Communication Control Toolkit (CCT) servers in a campus environment with one of the following:

- SIP-enabled contact center with an Avaya Communication Server 1000 PABX.
- SIP-enabled contact center with an Communication Manager and an Avaya Aura® SIP Enablement Services (SES) server.

Hot-standby and warm standby High Availability (HA) are configured in the same way using the High Availability Utility, but they perform differently because they depend on different technologies.

The level of Avaya Aura® Contact Center application High Availability you can achieve depends on your complete enterprise contact center solution. Avaya Aura® Contact Center also supports geographic disaster recovery and data resiliency.

High Availability (HA) supports resiliency for Contact Center Manager Server, Communication Control Toolkit, Contact Center Multimedia, and Contact Center Manager Administration.

One set of Contact Center applications (a Contact Center Manager Server, a CCT, a CCMA, and an optional CCMM) actively processes scripts and contacts. This set is called the active set. Another set of Contact Center applications, in the same contact center system, is running in standby mode. This standby set of Contact Center applications monitors and shadows active applications in the system but does not process calls. The standby CCMS monitors the active CCMS. The standby CCT monitors the active CCT. The standby CCMM monitors the active CCMM. Each active and standby pair of applications forms a resilient or replication pair. If any of the active applications fail the standby applications, running in standby mode, recognize this failure and start processing. The standby applications must be configured exactly the same as the active applications. Configuration changes made to the active system during normal operation are automatically copied to the standby applications. The standby applications are therefore configured correctly if they need to take over processing from the active systems. Statistical data is also automatically copied to the standby applications.

The standby CCMA is replicating the active CCMA server but CCMA services are not monitored. You must manually change over to the standby CCMA if the primary CCMA fails, since CCMA switchover is not automatic.

High Availability for CCMS, CCT and CCMM is configured using the High Availability utility in the Database Utilities. High Availability for CCMA is configured when you install CCMA.

High Availability is a licensed feature. It is enabled when a standby server license is purchased.

Prerequisites to Contact Center Server redundancy

- Install the active server. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- Install the standby server with the same configuration of drive letters and software, site name as the corresponding active server for Contact Center Manager Server,

Communication Control Toolkit, or Contact Center Multimedia. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).

Navigation

- Configuring warm standby or hot-standby managed IP address on page 539
- Configuring the warm standby or hot-standby server on page 541
- Configuring the notification of automatic switchovers on page 542
- Configuring warm standby or hot-standby manual switchovers on page 544
- Configuring service monitoring on page 544
- Configuring warm standby and hot-standby automatic switchovers on page 547
- Monitoring switchover information on page 547
- Reviewing shadowing on page 548
- Configuring Mission Critical High Availability on the Active Server on page 549
- Configuring Mission Critical High Availability on the Standby Server on page 551
- Starting a Mission Critical Active Server on page 553
- Starting shadowing on a Mission Critical Standby Server on page 553
- Stopping High Availability on a Mission Critical Standby Server on page 554
- Stopping High Availability on a Mission Critical Active Server on page 554
- Disabling Auto Startup on a Mission Critical server after reboot on page 555
- Selecting a startup mode on the Mission Critical Standby server after reboot on page 555
- Reinstating High Availability on page 556

Configuring warm standby or 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 Contact Center Manager Server, Communication Control Toolkit, or Contact Center Multimedia server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **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 **OK**.

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.

Name	Description
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 warm standby or hot-standby server

About this task

Configure the standby server for each Contact Center Manager Server, Communication Control Toolkit server or Contact Center Multimedia.

Procedure

1. Log on to the Contact Center Manager Server, Communication Control Toolkit, or Contact Center Multimedia server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **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. To configure a maximum time before the switchover occurs, select the **Switchover** check box, and select a time interval.
7. Click **OK**.

Important:

CCT Web services configuration information is not replicated to the stand-by server. Configure web services identically on both the CCT active server and the CCT standby 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	The length of time configured for server inactivity before the change to the Standby server for handling contacts.
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.

Configuring the notification of automatic switchovers

Before you begin

- Configure the standby server with automatic switchover. See Configuring warm standby or hot-standby managed IP address on page 539.
- If anonymous users are allowed, a username and password may not be required. Check with the Administrator of the e-mail server for setup configuration.

About this task

Use the High Availability utility to send an e-mail to a configured user.

Procedure

1. Log on to the Contact Center Manager Server, Communication Control Toolkit, or Contact Center Multimedia server.

2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **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 e-mail, in the **Hours** box, specify the number of hours to elapse between e-mail 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 **OK**.

Variable definitions

Name	Description
E-mail	Enable or disable e-mail notifications.
SMTP	SMTP server name this is automatically verified when saving the data.
Username	The E-mail User login name.
Password	The E-mail User login password.
Charset	The E-mail character set to use.
From Address	E-mail address from which to send notifications.
To Address	E-mail address to which to send notifications.
Hours	The interval, in hours, when an e-mail is sent to the configured user if an automatic switchover has occurred.

Configuring warm standby or hot-standby manual switchovers

Before you begin

- Configure the standby server for the Contact Center server (CCT, CCMS, or CCMM) you want to manually switchover. See Configuring warm standby or hot-standby managed IP address on page 539.

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.

Procedure

1. Log on to the current active Contact Center Manager Server, Communication Control Toolkit, or Contact Center Multimedia server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. In the left pane of the High Availability window, expand **Tasks**.
4. Double-click **CC Applications**.
5. In the first box, select the server to switchover.
6. Under **Enabled**, select **Yes**.
7. Under Switchover, select **Enabled**.
8. Click **Start**.

Configuring service monitoring

Before you begin

- Configure the standby server for each Contact Center server (CCT, CCMS) on which you want to configure automatic switchover. See Configuring warm standby or hot-standby managed IP address on page 539.

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 may, 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 coresident CCMS and CCT 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 is performed.

The following conditions must be met for switchover to occur:

If the switchover is not enabled, then all internal monitoring counters are reset and the monitoring restarts.

- Active and the Standby Server check boxes must be selected.
- A Valid license file and shadowing must be running.

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.

Procedure

1. Log on to the server for which you want to configure the automatic switchover for services that fail.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **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 Communication Control Toolkit 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 warm standby and hot-standby automatic switchovers

Before you begin

- Configure the standby server for each CCT, CCMS, or CCMM server on which you want to configure automatic switchover. See Configuring warm standby or hot-standby managed IP address on page 539.

About this task

Configure automatic switchover to automatically run the standby server if the active server fails or is shut down.

Procedure

1. Log on to the active server for which you want to configure the automatic switchover for services that fail.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **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 **OK**.

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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **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.
7. Click **Start**.

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 warm standby and hot-standby automatic switchovers on page 547.

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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. In the left pane of the High Availability window, expand **Configuration**.
4. Select **System**.
5. In the **System Configuration** panel, locate the shadowing entries.
6. Confirm the last record of shadowing is within the last minute of the current time.

7. Click **OK**.

Configuring Mission Critical High Availability on the Active Server

About this task

Configure High Availability resiliency on the Active Server using the High Availability Utility. The Active Server is the co-resident CCMS and CCT server that normally processes calls.

Procedure

1. Select one co-resident CCMS and CCT server to be the active server and log on.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **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 (Optional)** 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 **OK**.

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 switchover is made. 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.

Name	Description
Remote Geographic Node (Optional)	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 Co-resident CCMS and CCT Standby Server shadows the Active Server and takes over processing if the Active Server fails.

Procedure

1. Log on to the Standby Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **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 **OK**.

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 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 CCMS, CCT, and system processes.

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **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 CCMS and CCT 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 co-resident CCMS and CCT 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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
4. Expand **Configuration**.
5. Double-click **Server Mode**.
6. Under **Server Mode**, select **Non HA**.
7. Click **OK**.

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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
4. Expand **Configuration**.
5. Double-click **Server Mode**.
6. Under **Server Mode**, select **Non HA**.
7. Click **OK**.

Disabling Auto Startup on a Mission Critical server after reboot

About this task

Disable your Mission Critical server from automatically starting AACC 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**.

Reinstating 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. On the new active server, run the Database Maintenance utility and back up all of the database applications to a network share. You do not have to stop the active server to perform this back up.
2. On to the new standby server, if you are using Mission Critical HA, from the System Management and Monitoring Component (SMMC) system tray, click **Stop HA System**.

   If you are using Hot-standby HA or Warm-standby HA the server automatically stops shadowing.
3. Run the Database Maintenance utility and restore each database application individually from the network share.
4. Run the Server Configuration utility to update the Local CLAN information to identify the real local IP address.
5. If you are asked to reboot, a reboot of the server is not necessary.
6. In the Server Configuration utility, click **Apply All**.

7. Click **OK**.
8. Click **Exit**.
9. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
10. On the Server Mode dialog, click **OK**.
11. On the Save Data message box, click **Yes**.
12. Close HA configuration utility.
13. If you are using Mission Critical HA, skip to step 18 on page 557.
14. On the new standby server, click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
15. Under **Server Mode Configuration**, select **Switchover**.
16. Click **Tasks** > **System Control**.
17. Select **Shadowing**.
18. Click **Start**.
19. Click **OK** to close HA configuration utility.
20. On the new standby server, from the System Management and Monitoring Component (SMMC) system tray, click **Start HA System**.
21. On the new active server, from the System Management and Monitoring Component (SMMC) system tray, click **Enable Switchover**.

Chapter 61: Common procedures

This chapter describes the common procedures that you perform to administer your Avaya Aura® Contact Center software.

Navigation

- Starting or stopping Contact Center applications on page 559
- Stopping individual services on page 560
- Starting individual services on page 560
- Disabling services on page 561
- Enabling services on page 561

Starting or stopping Contact Center applications

Before you begin

Important:

When you start the System Control and Monitor Utility on a CCMA server, 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. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**.
3. Click the **Contact Center** tab.
4. Select the check box for each applications 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 **Stop Contact Center**.

Stopping individual services

Before you begin

- Know which server you are working on.
- Know which service or services you must stop.

About this task

During some procedures, you must stop one or more Windows services to manipulate a feature or function.

Procedure

1. Click **Start** > **Administrative Tools** > **Services**.
2. In the Services window, right-click the name of the service and click **Stop**.

Starting individual services

Before you begin

- Know which server you are working on.
- Know which service or services you must start.

About this task

During some procedures, you must start one or more Windows services to manipulate a feature or function.

Procedure

1. Click **Start** > **Administrative Tools** > **Services**.
2. In the Services window, right-click the name of the service and click **Start**.

Disabling services

Before you begin

- Know which server you are working on.
- Know which service or services you must disable.

About this task

During some procedures, you must disable one or more Windows services to manipulate a feature or function.

Procedure

1. Click **Start** > **Administrative Tools** > **Services**.
2. In the Services window, right-click the name of the service.
3. Click **Properties**.
4. From the Startup type list, choose **Disabled**.
5. Click **OK**.
6. Restart the computer.

Enabling services

Before you begin

- Know which server which you are working on.
- Know which service or services you must enable.

About this task

During some procedures, you must enable one or more Windows services to manipulate a feature or function.

Procedure

1. Click **Start** > **Administrative Tools** > **Services**.
2. In the Services window, right-click the name of the service.
3. Click **Properties**.
4. From the Startup type list, choose **Automatic**.

5. Click **OK**.
6. Restart the computer.

Appendix A: 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 CCMS, CCMA, CCT or CCMM server. However, this is time consuming, so Avaya recommends that you configure the final production name of the server before installing Contact Center software.

Important:

After you install Avaya Media Server software on a server, changing the server name or IP address is not supported.

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

- 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.

Server name or IP address change navigation

About this task

- Avaya Media Server server IP address or server name change on page 564
- CCMS server name change on page 565
- CCMS server IP address change on page 574
- Co-resident server name change on page 582
- Co-resident server IP address change on page 598
- CCMA server name change on page 607
- CCMA server IP address change on page 617
- CCT server name change on page 623
- CCT server IP address change on page 631
- CCMM server name change on page 635
- CCMM server IP address change on page 646

Avaya Media Server server IP address or server name change

After you install Avaya Media Server (Avaya MS) software on a server, changing the server name or IP address is not supported. If you need to rename the server or change the server IP address you must uninstall Avaya MS, change the server name or IP address, and reinstall and commission Avaya MS.

Changing the IP address or server name of the Avaya Media Server server

About this task

Change the name or IP address of a server with Avaya Media Server (Avaya MS) software installed to reflect the new server name.

Important:

To change the IP address or server name of the Avaya MS server, you must uninstall and reinstall the Avaya MS software. You must schedule a maintenance window for this procedure.

If the Avaya MS server is in a High Availability (HA) pair, performing this procedure disables HA. Stop both the Primary and the Backup servers before you start this procedure, and repeat the HA commissioning after you complete this procedure. For more information about HA commissioning, see *Avaya Aura® Contact Center Commissioning* (NN44400-312).

Procedure

1. Backup the Avaya MS database.

   For more information on how to backup the Avaya MS database, see *Avaya Aura® Contact Center Routine Maintenance* (NN44400-514).

2. Uninstall the Avaya MS software.

   For more information on how to uninstall the Avaya MS software, see *Avaya Aura® Contact Center Installation* (NN44400-311).

3. Change the server name or IP address.

4. Install Avaya MS software.

   For more information on how to install the Avaya MS software, see *Avaya Aura® Contact Center Installation* (NN44400-311).

5. Restore the Avaya MS database.

   For more information on how to restore the Avaya MS database, see *Avaya Aura® Contact Center Routine Maintenance* (NN44400-514).

CCMS server name change

Change the name of the Contact Center Manager Server and update the properties of the CCMS server on all of the 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 CCMS server name change

- 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 6 to 15 characters where the first character is alphabetical.
- Ensure that the new server name contains no underscores (_), spaces ( ), or punctuation.

CCMS server name change procedures

About this task

This task flow shows you the sequence of procedures you perform to change the name of the CCMS server. To link to any tasks, click on CCMS server name change navigation on page 567.

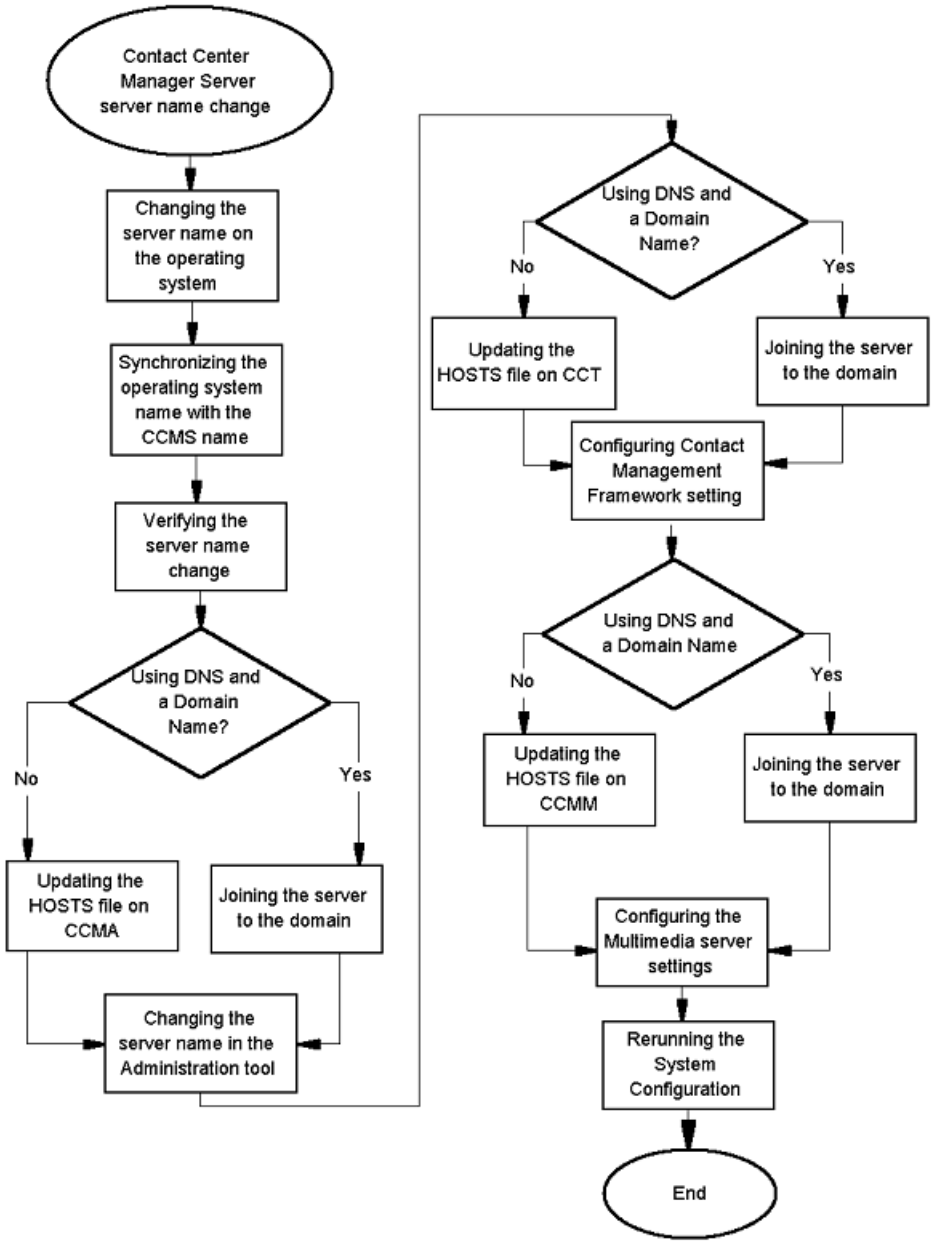


Figure 8: CCMS server name change procedures

CCMS server name change navigation

- Changing the server name on the operating system on page 568
- Synchronizing the operating system name with the CCMS name on page 569
- Verifying the server name change on page 569
- Updating the HOSTS file on page 570 (CCMA)

- Joining the server to the domain on page 571 (CCMA)
- Changing the server name in the Administration tool on page 571
- Updating the HOSTS file on page 570 (CCT)
- Joining the server to the domain on page 571 (CCT)
- Configuring the Contact Management Framework settings on page 572
- Updating the HOSTS file on page 570 (CCMM)
- Joining the server to the domain on page 571 (CCMM)
- Configuring the Multimedia server settings on page 572
- Rerunning the System Configuration on page 574

Changing the server name on the operating system

About this task

Change the server name on the Contact Center Manager Server operating system to reflect the new server name.

Procedure

1. Log on to the Contact Center Manager Server as administrator.
2. On the Contact Center Manager Server, choose **Start** > **Control Panel** > **System**.
3. In the **Computer name, domain, and workgroup settings** section, click **Change settings**.
4. Click the **Computer Name** tab.
5. Click **Change**.
6. Type the new server name.
7. Click **OK**.
8. 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 CCMS name. See Synchronizing the operating system name with the CCMS name on page 569.
9. If you use a Domain Name Service, contact your local network prime to update the DNS with the new server name.

Synchronizing the operating system name with the CCMS name

Before you begin

- Verify the server name change. See Verifying the server name change on page 593.

About this task

Synchronize the operating system name with the Contact Center Manager Server name to ensure that the Contact Center suite uses the new server name.

Procedure

1. Log on to the Contact Center Manager Server as administrator.
2. Close the **System Control and Monitor Utility** if it is running.
3. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **Computer Name Synchronisation Utility**.
4. Click **OK**.
   If the names do not match, you are prompted to synchronize the names.
5. After the Contact Center Manager Server services shut down and the synchronize process is complete, click **OK**.
6. On the Synchronization Utility box, click **OK**.
7. Restart the server.

Verifying the server name change

Before you begin

- Change the server name on the operating system. See Changing the server name on the operating system on page 568.

About this task

Verify that the Domain Name Service server or network has the correct server name.

Procedure

1. Click **Start** > **Run**.
2. Type `cmd`.
3. Click **OK**.
4. In a Command line window, type `ping <server name>`.

5. Verify that the IP address matches the IP address of the server with the new name.

Variable definitions

Name	Description
server name	The name of the Contact Center Manager 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 2008 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 2008 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.

Joining the server to the domain

About this task

If you are using a domain and a DNS, you join the server to the domain. This ensures that all servers can interpret the new server name.

Procedure

1. Log on to the server.
2. Change the server name or IP address.
3. Remove the server from the domain.
4. Join the server back to the domain using the new server name and IP address.

Changing the server name in the Administration tool

Before you begin

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name or that you updated the HOSTS file on the Contact Center Manager Administration server with the new Contact Center Manager Server name. See Updating the HOSTS file on page 570.

About this task

Change the Contact Center Manager Server name in the Administration tool to ensure that the connections in Contact Center Manager Administration connect to the correct server.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Log on to the Contact Center Manager Administration application as an administrator with all access permissions.
3. Click **Configuration**.
4. In the left pane, right-click the Contact Center Manager Server name to change.
5. Click **Edit Properties**.
6. Type the new server name, and click **Submit**.

Configuring the Contact Management Framework settings

Before you begin

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name and that you updated the HOSTS file on the Communication Control Toolkit server with the new Contact Center Manager Server name. See Updating the HOSTS file on page 570.
- Know how to restart the CCT services.

About this task

Update the Contact Management Framework component in Communication Control Toolkit with the new Contact Center Manager Server name to ensure that the contacts are routed correctly.

Procedure

1. Log on to the Communication Control Toolkit server.
2. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
3. Expand **CCT Admin**.
4. In the left pane, expand Communication Control Toolkit.
5. Expand **Server Configuration**.
6. Click the **Deployment Type** tab.
7. In the **CCMS Server Name** box, type the new name of the Contact Center Manager Server.
8. Click **Apply changes** to save the Contact Management Framework settings.
9. Click **OK** to close the window.
10. Restart the CCT services.

Configuring the Multimedia server settings

Before you begin

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name and that you updated the HOSTS file on the Contact Center

Multimedia server with the new Contact Center Manager Server name. See Updating the HOSTS file on page 570.

About this task

Configure the Multimedia server settings to ensure that the Multimedia database can find the contacts and has the correct name of the Contact Center Manager Server.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. 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 Web admin.
3. Choose **General Administration**.
4. Click **Server Settings**.
5. Select **Contact Center Manager Server**.
6. Click **Edit**.
7. In the **Server Name** box, change the name of the Contact Center Manager Server.
8. Click **Save**.
9. When the warning appears describing potential errors for changing this server, click **OK**.
10. If the **Contact Center Manager Server** server is installed on the same server as Contact Center Manager Server, in the Server Settings window, click **Contact Center License Server**.
11. Click **Edit**.
12. In the **Server Name** box, type the new name of the **Contact Center Manager Server** server.
13. Click **Save**.
14. If you have a backup Contact Center License Manager server, type the name in the **Backup Server** box.
15. Click **Save**.
16. When the warning appears, click **OK**.
17. Click **Yes** to restart the CCMM Services. This ensures that Multimedia contacts are routed to agents after changing the CCMS name.

Rerunning the System Configuration

Before you begin

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name and that you updated the HOSTS file on the Contact Center Multimedia server with the new Contact Center Manager Server name. See Updating the HOSTS file on page 570.

About this task

Rerun the System Configuration and restart the server Contact Center Manager Server to ensure that the CCMS server name change has been applied across the Contact Center suite.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center Manager Server**.
2. Choose **Server Configuration**.
3. Click **Apply All**.
4. Click **OK** to restart the system.

CCMS server IP address change

This section describes the steps you must perform to change the IP address of the Contact Center Manager Server.

CCMS server IP address change procedures

About this task

This task flow shows you the sequence of procedures you perform to change the IP address of the Contact Center Manager Server. To link to any tasks, click on CCMS server IP address change navigation on page 575.

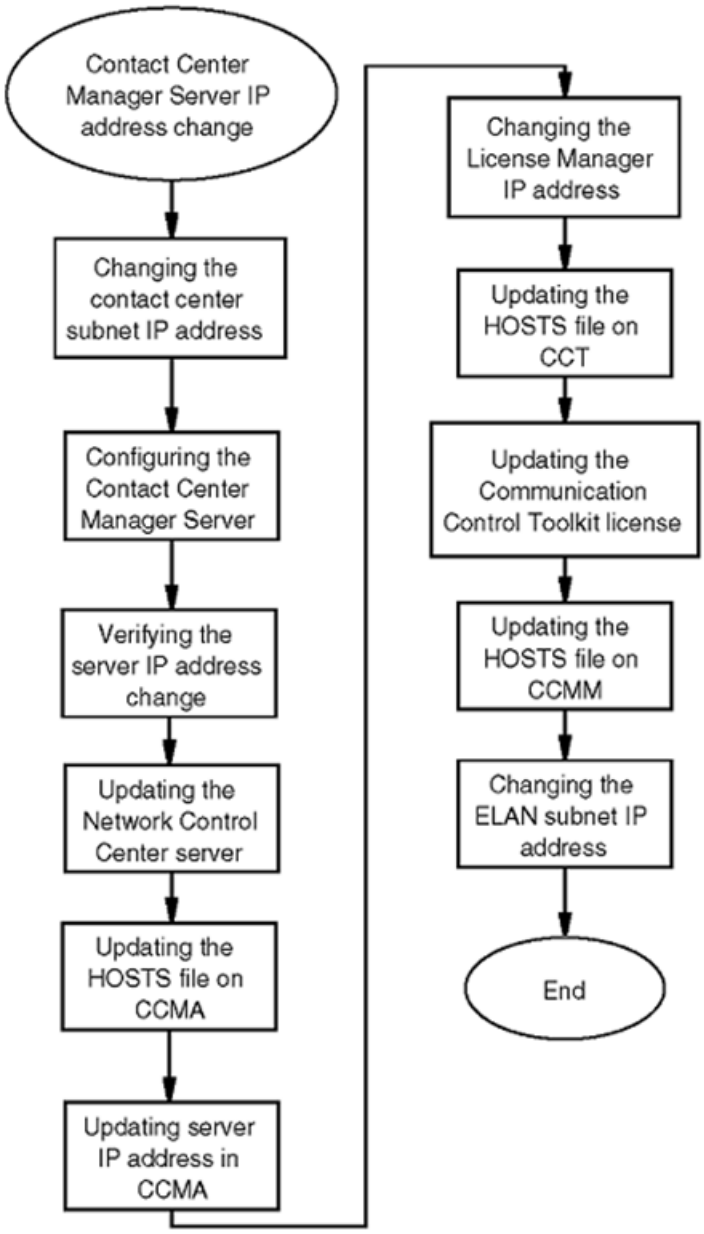


Figure 9: CCMS server IP address change procedures

CCMS server IP address change navigation

- Changing the contact center subnet IP address on page 576
- Configuring the Contact Center Manager Server on page 577

- Verifying the IP address change on page 577
- Updating the Network Control Center server on page 578
- Updating the HOSTS file on page 570 (CCMA)
- Updating the server IP address in CCMA on page 579
- Changing the Contact Center License Manager IP address on page 580
- Updating the HOSTS file on page 570 (CCT)
- Updating the Communication Control Toolkit license on page 581
- Updating the HOSTS file on page 570 (CCMM)
- Changing the ELAN subnet IP address on page 582

Changing the contact center subnet IP address

About this task

Change the contact center subnet IP address where the server IP address is recorded.

Procedure

1. Log on to the Contact Center Manager Server.
2. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**.
3. On the System Control and Monitor Utility window, click **Shutdown Contact Center**.
4. Choose **Start** > **Control Panel**.
5. Click **Network and Sharing Center**.
6. Click **Change adapter settings**.
7. Right-click the LAN connection of the contact center subnet network interface card, and then click **Properties**.
8. Select **Internet Protocol (TCP/IP)**, and then click **Properties**.
9. Type the new IP address, and then click **OK**.
10. In the Properties window, click **Close**.

Configuring the Contact Center Manager Server

Before you begin

- Change the contact center subnet IP address. See Changing the contact center subnet IP address on page 576.

About this task

You must perform the following steps to update the server IP address references in the Contact Center Manager Server.

Procedure

1. On the Contact Center Manager Server, choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
2. Click **Local Settings**.
3. Under **Contact Center Subnet**, in the **IP Address** box, type the new contact center subnet IP address.
4. If the Contact Center License Manager server is installed with Contact Center Manager Server, in the **Server Configuration** utility, click **Licensing**.
5. Under **License Server IP Address**, type the new Contact Center Manager Server IP address.

   Important:

   Type the new IP address only if the License package is Corporate. If License package is Nodal, the new IP is automatically updated.
6. Click **Apply All**.
7. Click **Yes** to restart the server.

Verifying the IP address change

Before you begin

- Configure the Contact Center Manager Server software with the new IP address. See Configuring the Contact Center Manager Server on page 577.

About this task

Verify that the Domain Name Service server or network has the correct server IP address.

Procedure

1. Click **Start** > **Run**.
2. Type `cmd`.
3. Click **OK**.
4. In a Command line window, type `ping <server name>`.
5. Verify that the IP address matches the new IP address of the server.

Variable definitions

Name	Description
server name	The name of the Contact Center Manager Server.

Updating the Network Control Center server

Before you begin

- Ensure that you have a network of Contact Center Manager Servers.
- Verify that the IP address changed. See Verifying the IP address change on page 577.

About this task

You must perform the following steps to update the Network Control Center server to ensure that it can identify the Contact Center Manager Server.

Procedure

1. On the Network Control Center server, choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Network Configuration**.
2. Click the **Site Table** tab.
3. On the **Site Table** tab, select the site name.
4. Click **Edit**.
5. In the **CLAN IP Address** box, type the new IP address.
6. Click **OK**.
7. On the **Nbconfig** dialog box, click **Verify**.
8. On the **Nbconfig** dialog box, click **OK**.

9. Verify that the correct IP address appears on the **Site Table** tab.
10. 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 2008 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 2008 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

Before you begin

- Change the server IP address. See Changing the contact center subnet IP address on page 576.

About this task

You must perform the following steps to update the server IP address references for Contact Center Manager Server in the Contact Center Manager Administration.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Log on to the Contact Center Manager Administration application as an administrator with all access permissions.
3. Click **Configuration**.
4. In the left pane, right-click the Contact Center Manager Server name to change.
5. Click **Edit Properties**.
6. Type the new server IP address, and click **Submit**.

Changing the Contact Center License Manager IP address

Before you begin

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server IP address, or you updated the HOSTS file on the Contact Center Manager Administration server with the new Contact Center Manager Server IP address. See Updating the HOSTS file on page 570.

About this task

If the Contact Center License Manager server is installed on the same server as Contact Center Manager Server, modify the primary or secondary Contact Center License Manager server IP address to ensure the entire Contact Center suite servers communicate the licensing information correctly.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Configuration**.
3. In the left pane, click **LM Service Configuration**.
4. In the right pane, click the **LM Service Configuration** icon.
5. In the **Primary License Manager Server's IP Address** box, type the new IP address.
6. Click **OK** to submit the information.
7. On the **Configuration Setup Completed** dialog box, click **OK**.
8. Click **Yes** to restart the Contact Center License Manager service.
9. Click **OK**.

10. On the **File** menu, click **Exit**.

Updating the Communication Control Toolkit license

Before you begin

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server IP address, or you updated the HOSTS file on the Communication Control Toolkit server with the new Contact Center Manager Server IP address. See Updating the HOSTS file on page 570.

About this task

If the Contact Center License Manager server is co-resident with the Contact Center Manager Server, use the following procedure to configure the Contact Center License Manager IP address for the Communication Control Toolkit server.

Procedure

1. Log on to the Communication Control Toolkit server.
2. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
3. Expand **CCT Admin**.
4. In the left pane, click **Communication Control Toolkit**.
5. Expand **Server Configuration**.
6. Click the **License Configuration** tab.
7. Under **Primary License Manager Server**, in the **IP Address** box, type the new IP address.
8. Click **Apply Changes** to save the new IP address.
9. On the **File** menu, click **Exit**.

Changing the ELAN subnet IP address

Before you begin

- Change the contact center subnet IP address. See Changing the contact center subnet IP address on page 576.

About this task

Change the ELAN subnet IP address to ensure that all servers on the network use the correct IP address for the Contact Center Manager Server.

Procedure

1. Log on to the Contact Center Manager Server.
2. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**.
3. On the System Control & Monitor Utility window, click **Shutdown Contact Center**.
4. On the Contact Center Manager Server, choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
5. Click the **Local Settings**.
6. Under **ELAN Subnet**, in the **IP Address** box, type the new ELAN subnet IP address.
7. Click **Apply All**.
8. Click **Yes** to restart the server.

Co-resident server name change

Change the name of the Co-resident server where Contact Center Manager Server and Contact Center Manager Administration 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 Co-resident server name change

- 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.

Co-resident server name change procedures

About this task

This task flow shows you the sequence of procedures you perform to change the name of the co-resident server. To link to any tasks, click on Co-resident server name change navigation on page 585.

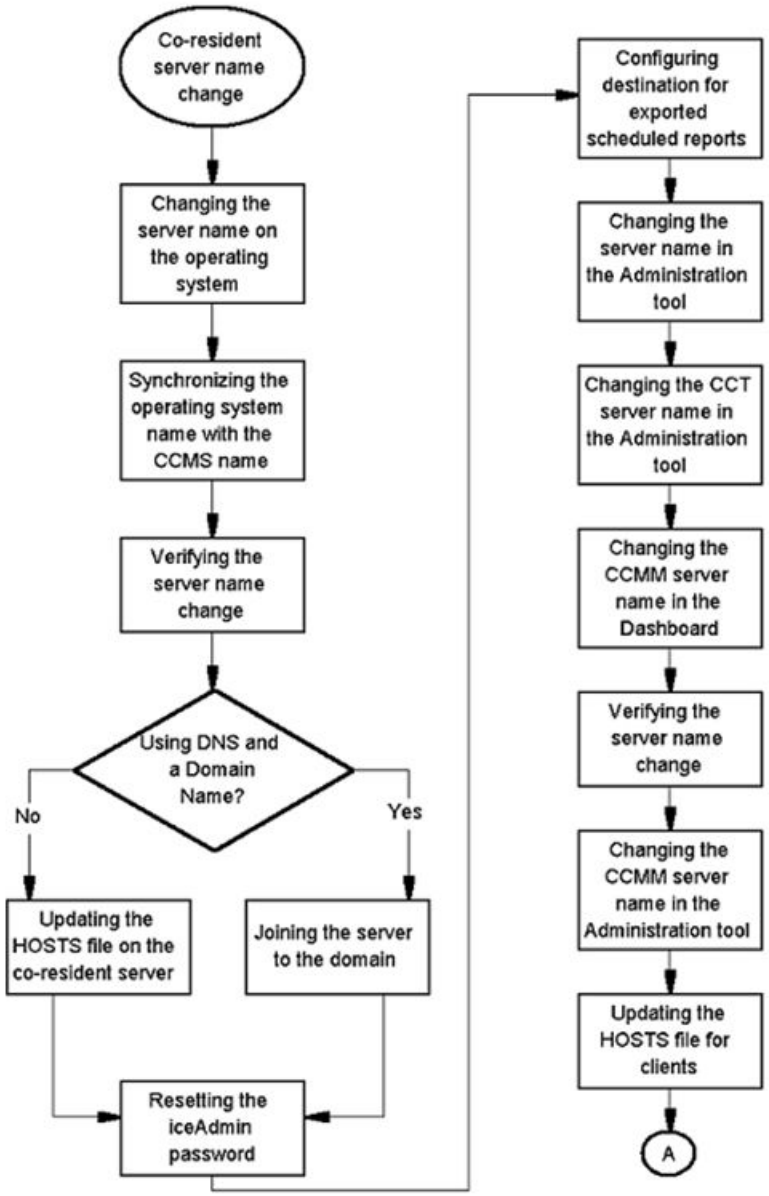


Figure 10: Co-resident server name change procedures

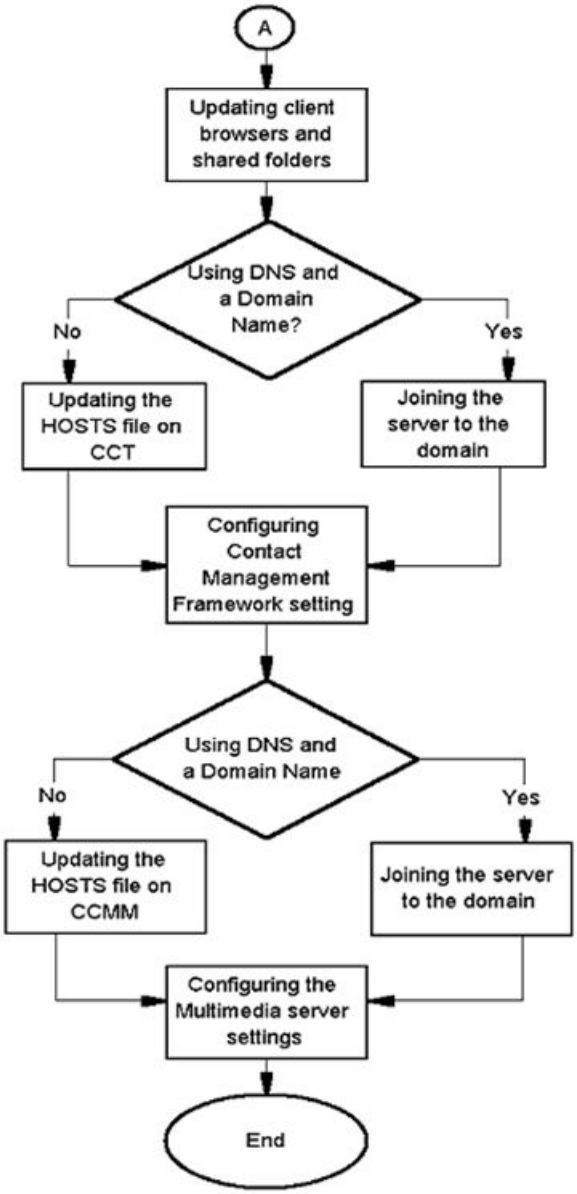


Figure 11: Co-Resident server name change procedures (continued)

Co-resident server name change navigation

- Changing the server name in the operating system on page 586
- Synchronizing the operating system name with the CCMS name on page 569
- Verifying the server name change on page 593

- Updating the HOSTS file on page 570 (on the co-resident server) **OR** Joining the server to the domain on page 571
- Resetting the iceAdmin password on page 589
- Configuring destination for exported scheduled reports on page 590
- Changing the server name in the Administration tool on page 571
- Changing the CCT server name in the Administration tool on page 591
- Changing the CCMM server name in the Dashboard on page 592
- Verifying the server name change on page 593
- Changing the CCMM server name in the Administration tool on page 593
- Updating the HOSTS file for clients on page 594
- Updating client browsers and shared folders on page 594
- Updating the HOSTS file on page 570 (on CCT) **OR** Joining the server to the domain on page 571
- Configuring the Contact Management Framework on page 596
- Updating the HOSTS file on page 570 (on CCMM) **OR** Joining the server to the domain on page 571
- Configuring the Multimedia server settings on page 572

Changing the server name in the operating system

About this task

Change the server name on the Contact Center Manager Server operating system to reflect the new name of the server.

Procedure

1. Log on to the Contact Center Manager Server as administrator.
2. On the Contact Center Manager Server, choose **Start** > **Control Panel** > **System**.
3. In the **Computer name, domain, and workgroup settings** section, click **Change settings**.
4. Click the **Computer Name** tab.
5. Click **Change**.
6. Type the new server name.
7. Click **OK**.
8. 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 CCMS name. See Synchronizing the operating system name with the CCMS name on page 569.

9. If you are using a Domain Name Service, contact your local network prime to update the DNS with the new server name.

Synchronizing the operating system name with the CCMS name

Before you begin

- Verify the server name change. See Verifying the server name change on page 593.

About this task

Synchronize the operating system name with the Contact Center Manager Server name to ensure that the Contact Center suite uses the new server name.

Procedure

1. Log on to the Contact Center Manager Server as administrator.
2. Close the **System Control and Monitor Utility** if it is running.
3. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **Computer Name Synchronisation Utility**.
4. Click **OK**.
   If the names do not match, you are prompted to synchronize the names.
5. After the Contact Center Manager Server services shut down and the synchronize process is complete, click **OK**.
6. On the Synchronization Utility box, click **OK**.
7. Restart the server.

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. Click **Start** > **Run**.
2. Type `cmd`.
3. Click **OK**.
4. In a Command line window, type `ping <server name>`.
5. Verify that the IP address matches the IP address of the server with the new name.

Variable definitions

Name	Description
server name	The name of the Contact Center Manager 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 2008 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 2008 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.

Joining the server to the domain

About this task

If you are using a domain and a DNS, you join the server to the domain. This ensures that all servers can interpret the new server name.

Procedure

1. Log on to the server.
2. Change the server name or IP address.
3. Remove the server from the domain.
4. Join the server back to the domain using the new server name and IP address.

Resetting the iceAdmin password

Before you begin

- Obtain the domain account name and password from your network administrator.

About this task

Reset the iceAdmin password to access the contents of the Administration database.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. On the **Start** menu, click **All Programs** > **Avaya** > **Contact Center** > **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 Contact Center Manager Administration 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

Configure the destination for exported scheduled reports if you export scheduled reports to a domain network computer.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Configuration**.
3. In the left pane, click **Avaya**.
4. Click **IceAdmin Password Change**.
5. In the **IceAdmin Password Change** dialog box, click **Domain Account**.
6. From the **Select Domain Name** list, select the name of the domain to add.
7. In the **Enter Domain Account** box, type the domain account.
8. In the **Enter Domain Account Password** box, type the domain account password.
9. In the **Confirm Domain Account Password** box, type the domain account password.

10. Click **OK**.
11. Click **OK**.

Changing the server name in the Administration tool

Before you begin

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name or that you updated the HOSTS file on the Contact Center Manager Administration server with the new Contact Center Manager Server name. See Updating the HOSTS file on page 570.

About this task

Change the Contact Center Manager Server name in the Administration tool to ensure that the connections in Contact Center Manager Administration connect to the correct server.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Log on to the Contact Center Manager Administration application as an administrator with all access permissions.
3. Click **Configuration**.
4. In the left pane, right-click the Contact Center Manager Server name to change.
5. Click **Edit Properties**.
6. Type the new server name, and click **Submit**.

Changing the CCT server name in the Administration tool

Before you begin

- Change the name of the Communication Control Toolkit. See Changing the server name on the operating system on page 625.

About this task

Update the CCT name in the CCMA configuration to ensure that the CCT Web admin launches correctly. Use the CCMA page to launch the CCT Web admin.

Procedure

1. Log on to the Contact Center Manager Administration server.

2. In a Web browser, start the CCMA browser.
3. Click **Configuration**.
4. From the **Server** menu, select **CCT Server**.
5. Right-click **CCT Server**, and then click **Edit Properties**.
6. Type the name of the new CCT Server.
   The system resolves the new CCT server name.
7. Click **Submit**.

Changing the CCMM server name in the Dashboard

Before you begin

- Change the name of the Contact Center Multimedia. See Changing the server name on the operating system on page 638.

About this task

Change the name of the Contact Center Multimedia server in the Dashboard to ensure that the CCMM Web admin launches properly.

Procedure

1. On the Contact Center Multimedia server, select **Start** > **All Programs** > **Avaya** > **Contact Center** > **Multimedia Server** > **Multimedia Dashboard**.
2. On the CCMM Dashboard, under **Server Availability**, right-click **Contact Center Manager Administration** and select **Edit**.
3. On the **Administrator Login** dialog, in the **User Name** box, type `GeneralAdmin`.
4. In the **Password** box, type the password. The default password is "__ccmm!".
5. Click **Login**.
6. On the **Administrator Login** dialog, in the text box, type the name for the current Contact Center Manager Administration server.
7. Click **Save**.

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. Click **Start** > **Run**.
2. Type `cmd`.
3. Click **OK**.
4. In a Command line window, type `ping <server name>`.
5. Verify that the IP address matches the IP address of the server with the new name.

Changing the CCMM server name in the Administration tool

Before you begin

- Change the name of the Contact Center Multimedia server. Changing the server name on the operating system on page 638.

About this task

Update the CCMM name in the CCMA configuration to ensure that the CCMM launches correctly.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. In a Web browser, start the CCMA browser.
3. Click **Configuration**.
4. From the **Server** menu, select **CCMM Server**.
5. Right-click **CCMM Server**, and then click **Edit Properties**.
6. Type the name of the new CCMM Server.
   The system resolves the new CCMM server name.

7. 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 PC.
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 file to reflect the new server..
5. On the **File** menu, click **Save**.
6. Close all windows.

Updating client browsers and shared folders

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 name or that you updated the HOSTS file on the clients with the new Contact Center Manager Server name. See Updating the HOSTS file for clients on page 594.

Important:

Administrators cannot update the browsers and shared folders for each user, therefore users needs to update their respective browsers and shared folders.

About this task

Update the client browsers and shared folders to reference the new Contact Center Manager Administration server name in the browser.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Log on to the Contact Center Manager Administration 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 Manager Administration server.
9. Click **Save Report**.
10. Click **Activate**.
11. Close the report.
12. Repeat step 4 on page 595 to step 11 on page 595 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 Management Framework

Before you begin

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name or that you updated the HOSTS file on the Communication Control Toolkit server with the new Contact Center Manager Server name. See Updating the HOSTS file on page 570.
- Know how to restart the CCT services.

About this task

Update the Contact Management Framework component in Communication Control Toolkit with the new Contact Center Manager Server name to ensure that the contacts are routed correctly.

Procedure

1. Log on to the Communication Control Toolkit server.
2. On the **Start** menu, choose **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
3. Expand **CCT Admin**.
4. In the left pane, expand Communication Control Toolkit.
5. Expand **Server Configuration**.
6. Click the **Deployment Type** tab.
7. In the **CCMS Server Name** box, type the new name of the Contact Center Manager Server.
8. Click **Apply Changes** to save the Contact Management Framework settings.
9. Click **OK** to close the window.
10. Restart the CCT services.

Configuring the Multimedia server settings

Before you begin

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server name and that you updated the HOSTS file on the Contact Center

Multimedia server with the new Contact Center Manager Server name. See Updating the HOSTS file on page 570.

About this task

Configure the Multimedia server settings to ensure that the Multimedia database can find the contacts and has the correct name of the Contact Center Manager Server.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. 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 Web admin.
3. Choose **General Administration**.
4. Click **Server Settings**.
5. Select **Contact Center Manager Server**.
6. Click **Edit**.
7. In the **Server Name** box, change the name of the Contact Center Manager Server.
8. Click **Save**.
9. When the warning appears describing potential errors for changing this server, click **OK**.
10. If the **Contact Center Manager Server** server is installed on the same server as Contact Center Manager Server, in the Server Settings window, click **Contact Center License Server**.
11. Click **Edit**.
12. In the **Server Name** box, type the new name of the **Contact Center Manager Server** server.
13. Click **Save**.
14. If you have a backup Contact Center License Manager server, type the name in the **Backup Server** box.
15. Click **Save**.
16. When the warning appears, click **OK**.
17. Click **Yes** to restart the CCMM Services. This ensures that Multimedia contacts are routed to agents after changing the CCMS name.

Co-resident server IP address change

Change the IP address of the Co-resident server where Contact Center Manager Server and Contact Center Manager Administration are installed on the same server and update the properties of all of the other servers in the Contact Center Suite.

Co-resident server IP address change procedures

About this task

This task flow shows you the sequence of procedures you perform to change the IP address of the co-resident server. To link to any tasks, click on Co-resident server IP address change navigation on page 599.

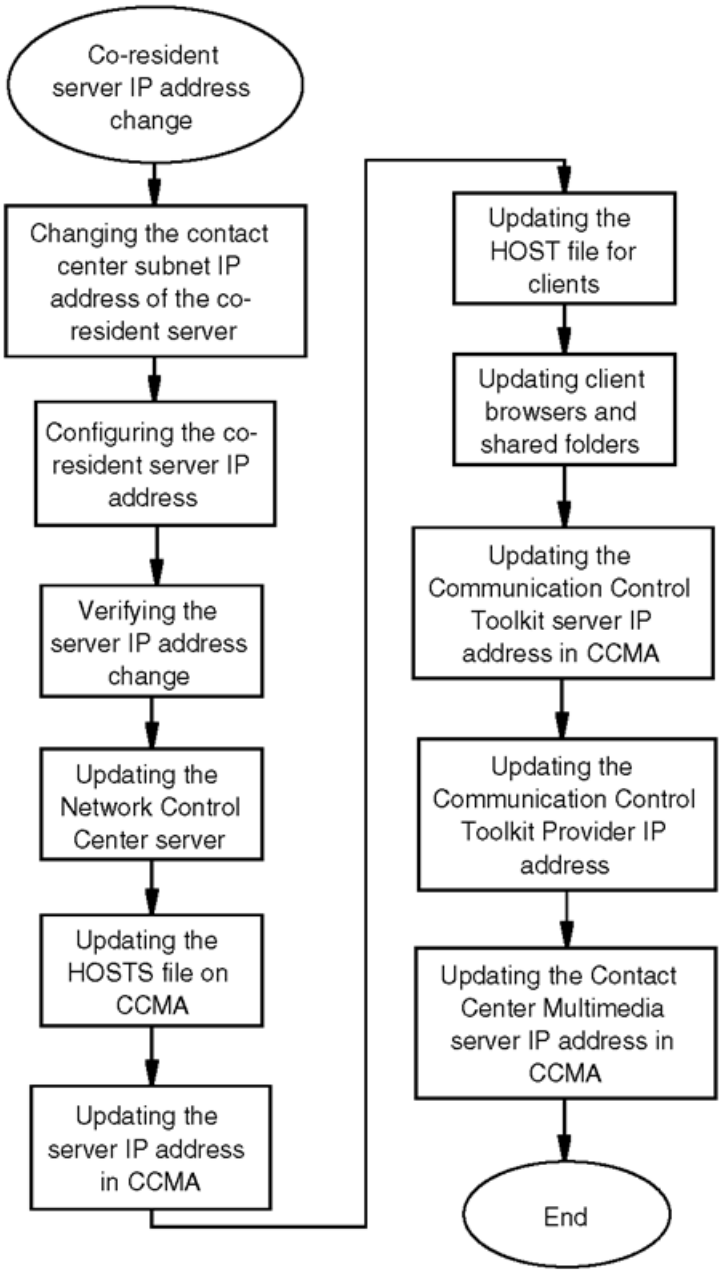


Figure 12: Co-resident server IP address change procedures

Co-resident server IP address change navigation

- Changing the contact center subnet IP address of the co-resident server on page 600
- Configuring the co-resident server IP address on page 601
- Verifying the server IP address change on page 601

- Updating the Network Control Center server on page 578
- Updating the HOSTS file on page 570 (CCMA)
- Updating the server IP address in CCMA on page 603
- Updating the HOSTS file for clients on page 594
- Updating client browsers and shared folders on page 594
- Updating the Communication Control Toolkit server IP address in CCMA on page 606
- Updating the Communication Control Toolkit provider IP address on page 606
- Updating the Contact Center Multimedia server IP address in CCMA on page 607

Changing the contact center subnet IP address of the co-resident server

About this task

You must perform the following steps to update the co-resident server IP address references.

Procedure

1. Log on to the co-resident server.
2. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**.
3. On the System Control & Monitor Utility window, click **Shutdown Contact Center**.
4. Choose **Start** > **Control Panel** > **Network and Internet** > **Network and Sharing Center**.
5. Click **Change adapter settings**.
6. Right-click the LAN connection of the contact center subnet network interface card, and then click **Properties**.
7. Select **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
8. Type the new IP address, and then click **OK**.
9. In the Properties window, click **Close**.

Configuring the co-resident server IP address

About this task

You must perform the following steps to update the co-resident server IP address references.

Procedure

1. Log on to the co-resident server.
2. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
3. Click the **Local Settings** tab.
4. Under **Avaya Server subnet**, type the new contact center subnet IP address.
5. If the Contact Center License Manager server is installed with Contact Center Manager Server, click the **Licensing** tab.
6. Ensure that the Primary Contact Center License Manager IP Address is the same as the new Contact Center Manager Server IP Address.
7. Click **Apply All**.
8. Click **Yes** to restart the server.

Verifying the server IP address change

Before you begin

- Configure the Contact Center Manager Server software with the new IP address. See Configuring the Contact Center Manager Server on page 577.

About this task

Verify that the Domain Name Service server or network has the correct server IP address.

Procedure

1. Click **Start** > **Run**.
2. Type `cmd`.
3. Click **OK**.
4. In a Command line window, type `ping <server name>`.

5. Verify that the IP address matches the new IP address of the server.

Variable definitions

Name	Description
server name	The name of the Contact Center Manager Server.

Updating the Network Control Center server

Before you begin

- Ensure that you have a network of Contact Center Manager Servers.
- Verify that the IP address changed. See Verifying the IP address change on page 577.

About this task

You must perform the following steps to update the Network Control Center server to ensure that it can identify the Contact Center Manager Server.

Procedure

1. On the Network Control Center server, choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Network Configuration**.
2. Click the **Site Table** tab.
3. On the **Site Table** tab, select the site name.
4. Click **Edit**.
5. In the **CLAN IP Address** box, type the new IP address.
6. Click **OK**.
7. On the **Nbconfig** dialog box, click **Verify**.
8. On the **Nbconfig** dialog box, click **OK**.
9. Verify that the correct IP address appears on the **Site Table** tab.
10. 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 2008 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 2008 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

Before you begin

- Change the server IP address. See Changing the contact center subnet IP address of the co-resident server on page 600.

About this task

You must perform the following steps to update the server IP address references for Contact Center Manager Server in the Contact Center Manager Administration.

Procedure

1. On the co-resident server, log on to the Contact Center Manager Administration application 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 PC.
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 file to reflect the new server..
5. On the **File** menu, click **Save**.
6. Close all windows.

Updating client browsers and shared folders

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 name or that you updated the HOSTS file on the clients with the new Contact Center Manager Server name. See Updating the HOSTS file for clients on page 594.

Important:

Administrators cannot update the browsers and shared folders for each user, therefore users needs to update their respective browsers and shared folders.

About this task

Update the client browsers and shared folders to reference the new Contact Center Manager Administration server name in the browser.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Log on to the Contact Center Manager Administration 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 Manager Administration server.
9. Click **Save Report**.
10. Click **Activate**.
11. Close the report.
12. Repeat step 4 on page 605 to step 11 on page 605 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 co-resident 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**.

Updating the Communication Control Toolkit provider IP address

About this task

In a contact center environment, update the IP address for the Communication Control Toolkit (CCT) provider in the CCT Web admin so CCT can control voice contacts.

Procedure

1. On the co-resident server, add the page: http:\\<*new CCT 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**, type the new IP address for the provider.
9. Click **Save**.

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 co-resident 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**.

CCMA server name change

Change the name of the Contact Center Manager Administration and update the properties of all of the 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.

If the CCMA server is in a domain, and has CCMA replication configured, perform the name change with the server in the domain.

Prerequisites for CCMA server name change

- The name cannot be the same as any other computer or domain name in the network.
- The name must contain 6 to 15 characters (A through Z, 0 through 9).
- The first character of the name must be alphabetical.
- No other characters are allowed. For example, the name cannot include underscores (_).

CCMA server name change procedures

About this task

This task flow shows you the sequence of procedures you perform to change the name of the Contact Center Manager Administration server. To link to any tasks, click on CCMA server name change navigation on page 609.

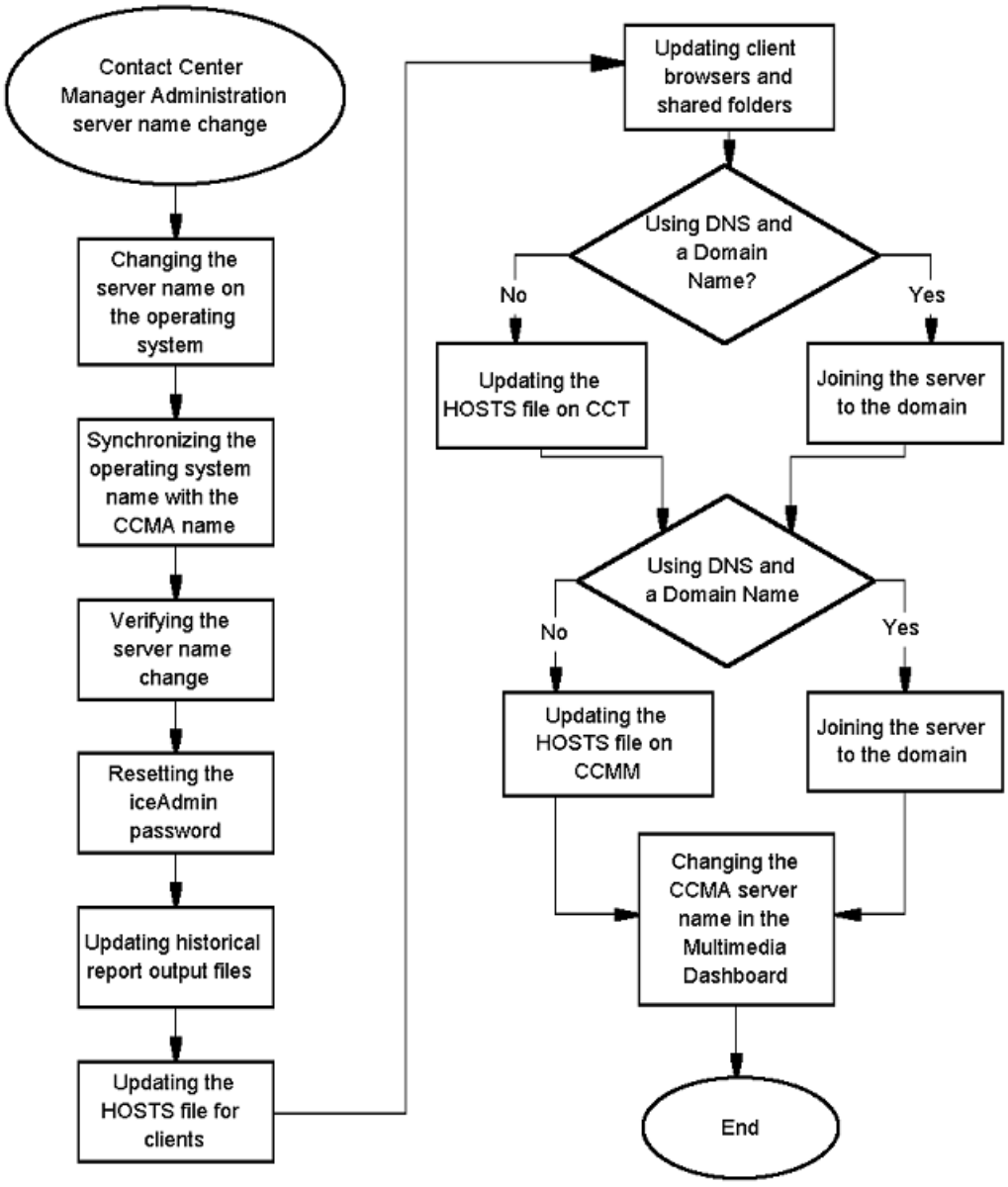


Figure 13: CCMA server name change procedures

CCMA server name change navigation

- Changing the server name in the operating system on page 610
- Synchronizing the operating system name with the CCMA name on page 611
- Verifying the server name change on page 593
- Resetting the iceAdmin password on page 589

- Updating historical report output files on page 613
- Updating the HOSTS file for clients on page 594
- Updating client browsers and shared folders on page 614
- Updating the HOSTS file on page 570 (CCT) **OR** Joining the server to the domain on page 571
- Updating the HOSTS file on page 570 (CCMM) **OR** Joining the server to the domain on page 571
- Changing the CCMA server name in the Multimedia Dashboard on page 616

Changing the server name in the operating system

About this task

Change the name of the Contact Center Manager Administration server in the operating system to indicate the name of the server.

Procedure

1. On the Contact Center Manager Administration server, select **Start** > **Control Panel** and then click **System**.
2. In the **Computer name, domain, and workgroup setting** section, click **Change settings**.
3. Click the **Computer Name** tab.
4. Click **Change**.
5. In the **Computer Name Changes** dialog box, in the **Computer Name** box, type the new server name.
6. Click **OK**.
7. 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 CCMS name. See Synchronizing the operating system name with the CCMA name on page 611.
8. If you use a Domain Name Service, contact your local network prime to update the DNS with the new server name.

Synchronizing the operating system name with the CCMA name

Before you begin

- Verify the server name change. See Verifying the server name change on page 593.

About this task

Synchronize the operating system name with the Contact Center Manager Administration name to ensure that the Contact Center suite uses the new server name.

Procedure

1. Log on to the Contact Center Manager Administration as administrator.
2. Close the **System Control and Monitor Utility** if it is running.
3. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **Computer Name Synchronisation Utility**.
4. Click **OK**.
   If the names do not match, you are prompted to synchronize the names.
5. After the Contact Center Manager Administration services shut down and the synchronize process is complete, click **OK**.
6. On the Synchronization Utility box, click **OK**.
7. Restart the server.

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. Click **Start** > **Run**.
2. Type `cmd`.
3. Click **OK**.
4. In a Command line window, type `ping <server name>`.

5. Verify that the IP address matches the IP address of the server with the new name.

Variable definitions

Name	Description
server name	The name of the Contact Center Manager Administration.

Resetting the iceAdmin password

Before you begin

- Obtain the domain account name and password from your network administrator.

About this task

Reset the iceAdmin password to access the contents of the Administration database.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. On the **Start** menu, click **All Programs** > **Avaya** > **Contact Center** > **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 Contact Center Manager Administration 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**.

Updating historical report output files

Before you begin

- Plan to export scheduled reports to a computer on your domain network.

About this task

Configure the destination for exported scheduled reports if you export scheduled reports to a domain network computer.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Configuration**.
3. In the left pane, click **Avaya**.
4. Click **IceAdmin Password Change**.
5. In the **IceAdmin Password Change** dialog box, click **Domain Account**.
6. From the **Select Domain Name** list, select the name of the domain to add.
7. In the **Enter Domain Account** box, type the domain account.
8. In the **Enter Domain Account Password** box, type the domain account password.
9. In the **Confirm Domain Account Password** box, type the domain account password.
10. Click **OK**.
11. Click **OK**.

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 PC.
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 file to reflect the new server..
5. On the **File** menu, click **Save**.
6. Close all windows.

Updating client browsers and shared folders

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 Administration name or that you updated the HOSTS file on the clients with the new Contact Center Manager Administration name. See Updating the HOSTS file for clients on page 594.

Important:

Administrators cannot update the browsers and shared folders for each user, therefore users needs to update their respective browsers and shared folders.

About this task

Update the client browsers and shared folders to reference the new Contact Center Manager Administration server name in the browser.

Procedure

1. Log on to the Contact Center Manager Administration server.

2. Log on to the Contact Center Manager Administration application as an administrator with full 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, select that report.
6. 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 Manager Administration server.
9. Click **Save Report**.
10. Click **Activate**.
11. Close the report.
12. Repeat step 4 on page 615 to step 11 on page 615 for each report.

Variable definitions

Name	Description
Output path	The path of the file where the historical reports are stored. The path format is \\ [computer name]\[shared folder name]\[file name].

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 2008 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 2008 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.

Joining the server to the domain

About this task

If you are using a domain and a DNS, you join the server to the domain. This ensures that all servers can interpret the new server name.

Procedure

1. Log on to the server.
2. Change the server name or IP address.
3. Remove the server from the domain.
4. Join the server back to the domain using the new server name and IP address.

Changing the CCMA server name in the Multimedia Dashboard

Before you begin

- Change the name of the Contact Center Multimedia. See Changing the server name in the operating system on page 610.

About this task

Change the name of the Contact Center Manager Administration server in the Dashboard to ensure that the CCMA Web admin launches properly.

Procedure

1. On the Contact Center Multimedia server, select **Start** > **All Programs** > **Avaya** > **Contact Center** > **Multimedia Server** > **Multimedia Dashboard**.
2. In the **Server Availability** area, select the old CCMA name.
3. Right-click **CCMA Server**, and then click **Edit**.
4. Type the username and password, and then click **Login**.
5. Type the new CCMA server name, and click **OK**.
6. Close the Dashboard window.

CCMA server IP address change

Change the IP address of the Contact Center Manager Administration server and update the properties of all other servers in the Contact Center Suite. If the CCMA server is in a domain, and has ADAM replication configured, perform the IP address change with the server in the domain.

CCMA server IP address change procedures

About this task

This task flow shows you the sequence of procedures you perform to change the Contact Center Manager Administration server IP address. To link to any tasks, click on CCMA server IP address change navigation on page 618.

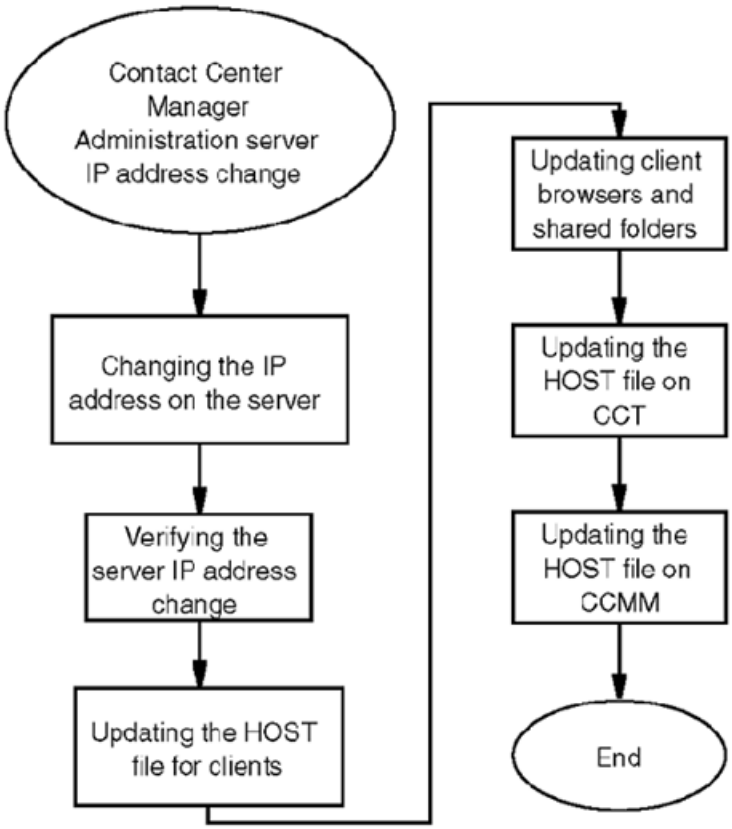


Figure 14: CCMA server IP address change procedures

CCMA server IP address change navigation

- Changing the server IP address on the server on page 618
- Verifying the server IP address change on page 619
- Updating the HOSTS file for clients on page 594
- Updating client browsers and shared folders on page 614
- Updating the HOSTS file on page 570 (CCT)
- Updating the HOSTS file on page 570 (CCMM)

Changing the server IP address on the server

About this task

You must perform the following steps to update the server IP address references for the Contact Center Manager Server in the Contact Center Manager Administration software.

Procedure

1. On the Contact Center Manager Administration Server, stop the services.
2. From the **Start** menu, choose **Control Panel**.
3. Click **Network and Internet** > **Network Sharing Center**.
4. Click **Change adapter settings**.
5. Right-click **Network Connections**.
6. Right-click the LAN connection, and then click **Properties**.
7. Select **Internet Protocol Version 4 (TCP/IP)**, and then click **Properties**.
8. In the **IP Address** box, type the new IP address.
9. Click **OK**.
10. On the Properties window, click **Close**.
11. Restart the services.

Verifying the server IP address change

Before you begin

- Configure the Contact Center Manager Administration software with the new IP address.

About this task

Verify that the Domain Name Service server or network has the correct server IP address.

Procedure

1. Click **Start** > **Run**.
2. Type `cmd`.
3. Click **OK**.
4. In a Command line window, type `ping <server name>`.
5. Verify that the IP address matches the new IP address of the server.

Variable definitions

Name	Description
server name	The name of the Contact Center Manager Administration.

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 PC.
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 file to reflect the new server..
5. On the **File** menu, click **Save**.
6. Close all windows.

Updating client browsers and shared folders

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 Administration name or that you updated the HOSTS file on the clients with the new Contact Center Manager Administration name. See Updating the HOSTS file for clients on page 594.

Important:

Administrators cannot update the browsers and shared folders for each user, therefore users needs to update their respective browsers and shared folders.

About this task

Update the client browsers and shared folders to reference the new Contact Center Manager Administration server name in the browser.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Log on to the Contact Center Manager Administration application as an administrator with full 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, select that report.
6. 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 Manager Administration server.
9. Click **Save Report**.
10. Click **Activate**.
11. Close the report.
12. Repeat step 4 on page 621 to step 11 on page 621 for each report.

Variable definitions

Name	Description
Output path	The path of the file where the historical reports are stored. The path format is \\ [computer name]\[shared folder name]\[file name].

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 2008 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 2008 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.

CCT server name change

Change the name of the Communication Control Toolkit 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 CCT server name change

- 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 where the first character is alphabetical.
- Ensure that the new server name contains no underscores (_), spaces ( ), or punctuation.

CCT server name change procedures

About this task

This task flow shows you the sequence of procedures you perform to change the name of the Communication Control Toolkit server. To link to any tasks, click on CCT server name change navigation on page 624.

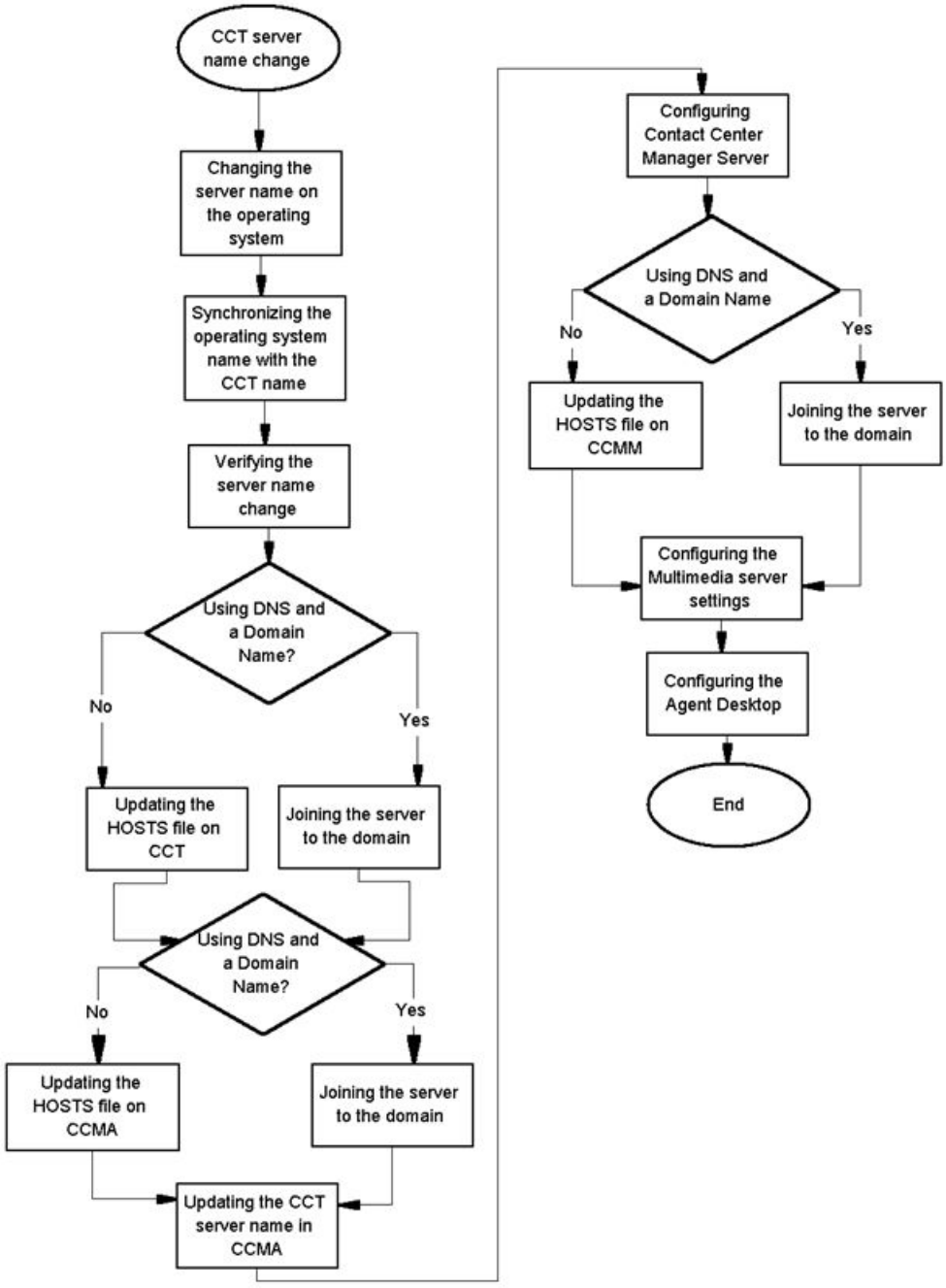


Figure 15: CCT server name change procedures

CCT server name change navigation

- Changing the server name on the operating system on page 625
- Synchronizing the operating system name with the CCT name on page 626

- Verifying the server name change on page 593
- Updating the HOSTS file on page 570 (CCT) **OR** Joining the server to the domain on page 571
- Updating the HOSTS file on page 570 (CCMA) **OR** Joining the server to the domain on page 571
- Updating the CCT server name in CCMA on page 628
- Configuring Contact Center Manager Server on page 629
- Updating the HOSTS file on page 570 (CCMM) **OR** Joining the server to the domain on page 571
- Configuring the Multimedia server settings on page 629
- Configuring the Agent Desktop on page 630

Changing the server name on the operating system

Before you begin

- Know how to restart the Communication Control Toolkit services.

About this task

Change the Communication Control Toolkit server name on the operating system to ensure that the server has the correct name and other servers in Contact Center can locate it.

Procedure

1. On the Communication Control Toolkit Server, choose **Start** > **Control Panel** > **System**.
2. In the **Computer name, domain, and workgroup settings** section, click **Change settings**.
3. Click the **Computer Name** tab.
4. Click **Change**.
5. Type the new server name.
6. Click **OK**.
7. 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 CCT name. See Synchronizing the operating system name with the CCT name on page 626.

8. If you use a Domain Name Service, contact your local network prime to update the DNS with the new server name.

Synchronizing the operating system name with the CCT name

Before you begin

- Verify the server name change. See Verifying the server name change on page 593.

About this task

Synchronize the operating system name with the Communication Control Toolkit name to ensure that the Contact Center suite uses the new server name.

Procedure

1. Log on to the Communication Control Toolkit as administrator.
2. Close the **System Control and Monitor Utility** if it is running.
3. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **Computer Name Synchronisation Utility**.
4. Click **OK**.
   If the names do not match, you are prompted to synchronize the names.
5. After the Communication Control Toolkit services shut down and the synchronize process is complete, click **OK**.
6. On the **Synchronisation Utility** box, click **OK**.
7. Restart the server.
8. After the server has rebooted, ensure that the NCCT DALS service is running.
9. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
10. In **Server** – **Configuration Deployment Type** select a different deployment type and then select the original deployment type again. This is done to enable the **Apply Changes** button.
11. Click **Apply Changes**.
12. Restart the CCT services.

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. Click **Start** > **Run**.
2. Type `cmd`.
3. Click **OK**.
4. In a Command line window, type `ping <server name>`.
5. Verify that the IP address matches the IP address of the server with the new name.

Variable definitions

Name	Description
server name	The name of the Communication Control Toolkit.

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 2008 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 2008 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.

Joining the server to the domain

About this task

If you are using a domain and a DNS, you join the server to the domain. This ensures that all servers can interpret the new server name.

Procedure

1. Log on to the server.
2. Change the server name or IP address.
3. Remove the server from the domain.
4. Join the server back to the domain using the new server name and IP address.

Updating the CCT server name in CCMA

Before you begin

- Change the name of the Communication Control Toolkit. See Changing the server name on the operating system on page 625.

About this task

Update the CCT name in the CCMA configuration to ensure that the CCT Web admin launches correctly. Use the CCMA page to launch the CCT Web admin.

Procedure

1. Log on to the Contact Center Manager Administration server.

2. In a Web browser, start the CCMA browser.
3. Click **Configuration**.
4. From the **Server** menu, select **CCT Server**.
5. Right-click **CCT Server**, and then click **Edit Properties**.
6. Type the name of the new CCT Server.
   The system resolves the new CCT server name.
7. Click **Submit**.

Configuring Contact Center Manager Server

Before you begin

- Change the name of the Communication Control Toolkit server in the operating system. See Changing the server name on the operating system on page 625.

About this task

Configure the Contact Center Manager Server software with the name of the new Communication Control Toolkit to ensure that Communication Control Toolkit works correctly.

Procedure

1. On the Contact Center Manager Server, select **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
2. Click the **CCT Server** tab.
3. In the **CCT Host Name** box, type the new name of the Communication Control Toolkit server.
4. Click **Apply All**.
5. Restart the server when you are prompted to do so.

Configuring the Multimedia server settings

Before you begin

- Ensure that the Domain Name Service server is updated with the new Communication Control Toolkit name or that you updated the HOSTS file on the Contact Center Multimedia

server with the new Communication Control Toolkit name. See Updating the HOSTS file on page 570.

About this task

Configure the Multimedia server settings to ensure that the Multimedia database can find the contacts and has the correct name of the Communication Control Toolkit.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. Choose **General Administration**.
3. Click **Server Settings**.
4. Select Communication Control Toolkit.
5. Click **Edit**.
6. In the **Server Name** box, change the name of the Communication Control Toolkit.
7. Click **Save**.
8. When the warning appears, click **OK**.
9. Click **Yes** to restart the CCMM Services. This ensures that Multimedia contacts are routed to agents after changing the CCMS name.

Configuring the Agent Desktop

Before you begin

- Ensure that agents use the Agent Desktop.
- Change the name of the Communication Control Toolkit server in the operating system. See Changing the server name on the operating system on page 625.

About this task

Configure the Avaya Aura® Agent Desktop if you use the Agent Desktop with the Communication Control Toolkit to allow agents to monitor calls and make calls using the telephony toolbar.

Procedure

1. Log on to the Communication Control Toolkit server.
2. In Windows Explorer, navigate to Avaya\Contact Center Multimedia\Agent Desktop.
3. Open the CCADAppSettings.xml file in Notepad.
4. Locate the CCTSERVER key in the CCADAppSettings.xml file.

5. Change the name of the server key to the new Communication Control Toolkit server name.
6. Save the file.

CCT server IP address change

Change the IP address of the Communication Control Toolkit server and update the properties of all other servers in the Contact Center Suite.

CCT server IP address change procedures

About this task

This task flow shows you the sequence of procedures you perform to change the IP address of the Communication Control Toolkit server. To link to any tasks, click on CCT server IP address change navigation on page 632.

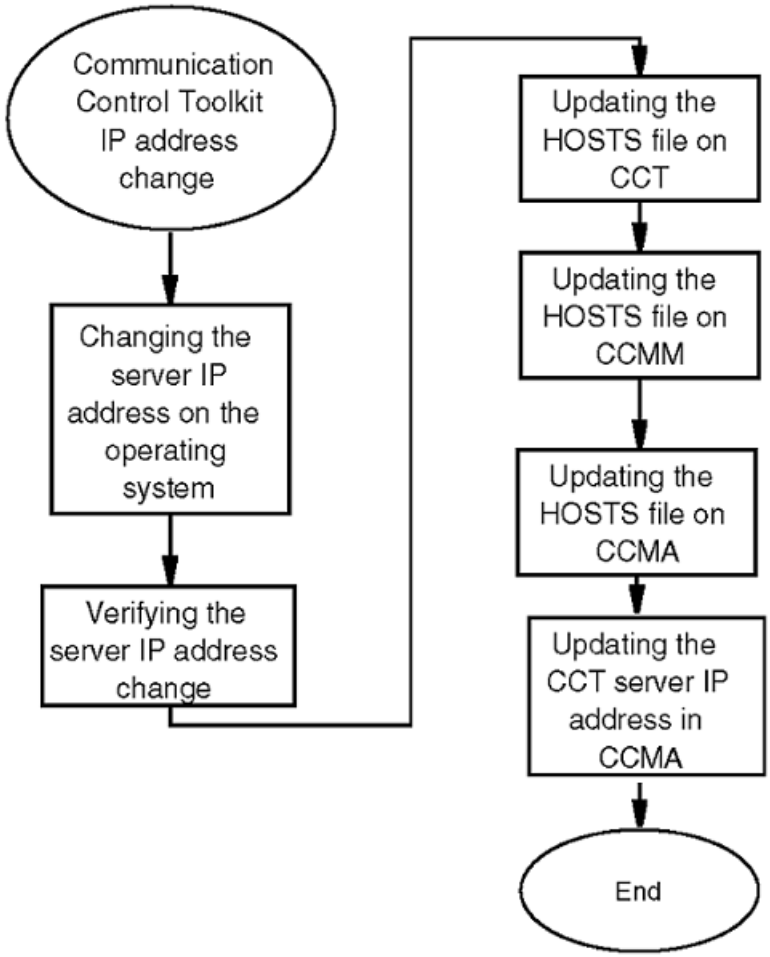


Figure 16: CCT server IP address change procedures

CCT server IP address change navigation

- Changing the server IP address on the operating system on page 633
- Verifying the server IP address change on page 633
- Updating the HOSTS file on page 570 (CCT)
- Updating the HOSTS file on page 570 (CCMM)
- Updating the HOSTS file on page 570 (CCMA)
- Updating the CCT server IP address in CCMA on page 635

Changing the server IP address on the operating system

Before you begin

- Know how to restart the Communication Control Toolkit services.

About this task

Change the Communication Control Toolkit 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. On the Communication Control Toolkit Server, stop the services.
2. From the **Start** menu, choose **Control Panel**.
3. Click **Network and Internet** > **Network Sharing Center**.
4. Click **Change adapter settings**.
5. Right-click **Network Connections**.
6. Right-click the LAN connection, and then click **Properties**.
7. Select **Internet Protocol Version 4 (TCP/IP)**, and then click **Properties**.
8. In the **IP Address** box, type the new IP address.
9. Click **OK**.
10. On the Properties window, click **Close**.
11. Restart the services.

Verifying the server IP address change

Before you begin

- Configure the Communication Control Toolkit software with the new IP address.

About this task

Verify that the Domain Name Service server or network has the correct server IP address.

Procedure

1. Click **Start** > **Run**.
2. Type `cmd`.

3. Click **OK**.
4. In a Command line window, type `ping <server name>`.
5. Verify that the IP address matches the new IP address of the server.

Variable definitions

Name	Description
server name	The name of the Communication Control Toolkit 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 2008 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 2008 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 CCT server IP address in CCMA

Before you begin

- Change the name of the Communication Control Toolkit. See Changing the server name on the operating system on page 625.
- Update the name of the new CCT server in CCMA. See Updating the CCT server name in CCMA on page 628.

About this task

Update the CCT IP address in the CCMA configuration to ensure that the CCT Web admin launches correctly. Use the CCMA page to launch the CCT Web admin.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. In a Web browser, start the CCMA browser.
3. Click **Configuration**.
4. From the **Server** menu, select **CCT Server**.
5. Right-click **CCT Server**, and then click **Edit Properties**.
6. Type the name of the new CCT Server to resolve the new CCT server IP address.
7. Click **Submit**.

CCMM server name change

Change the name of the Contact Center Multimedia 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 CCMM server name change

- 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.

CCMM server name change procedures

About this task

This task flow shows you the sequence of procedures you perform to change the name of the Contact Center Multimedia server. To link to any tasks, click on CCMM server name change navigation on page 637.

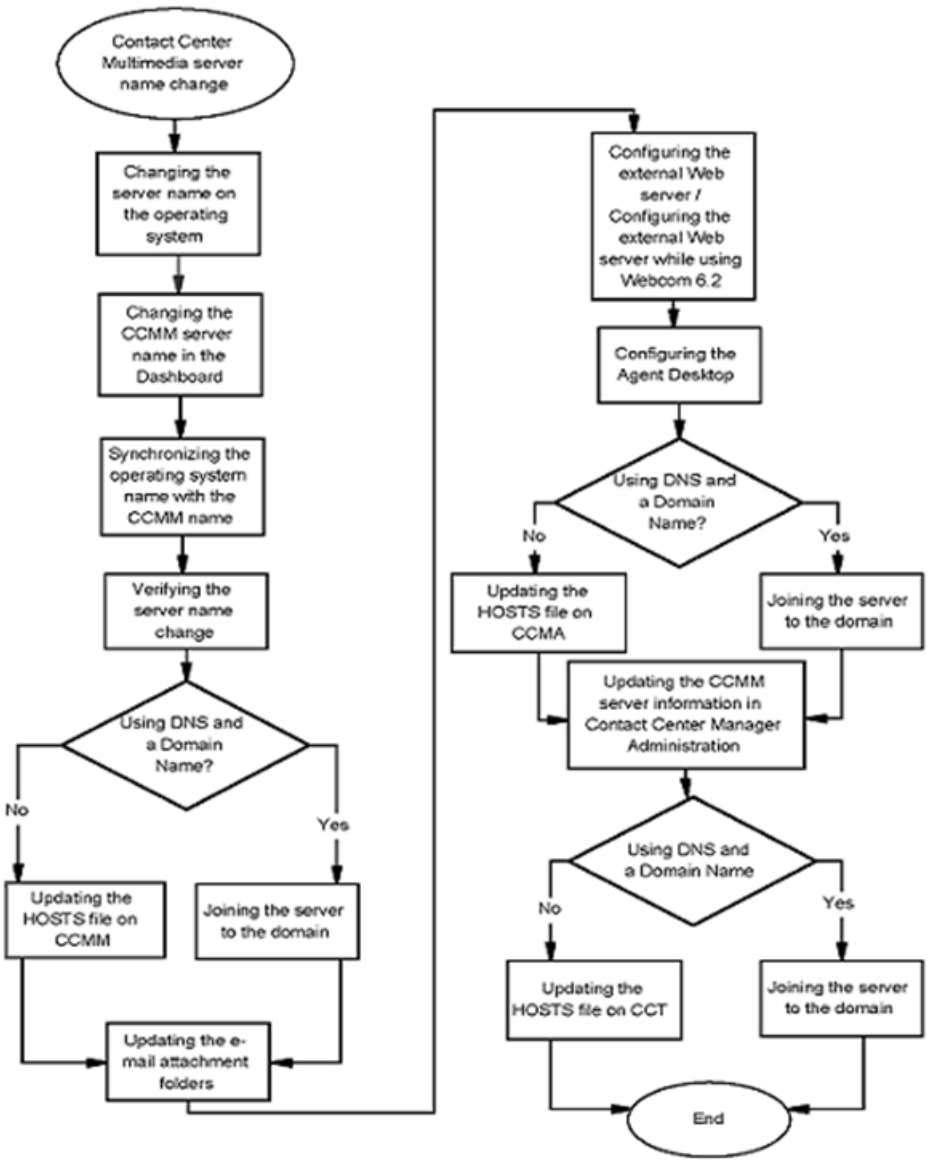


Figure 17: CCMM server name change procedures

CCMM server name change navigation

- Changing the server name on the operating system on page 638
- Changing the CCMM server name in the Dashboard on page 592
- Synchronizing the operating system name with the CCMM name on page 639
- Verifying the server name change on page 593

- Updating the HOSTS file on page 570 (CCMM) **OR** Joining the server to the domain on page 571
- Updating the e-mail attachment folders on page 642
- Configuring the external Web server on page 642
- Configuring the external Web server while using Webcom 6.2 (xampp 1.7.3 or higher) on page 644
- Configuring the Agent Desktop on page 644
- Updating the HOSTS file on page 570 (CCMA) **OR** Joining the server to the domain on page 571
- Updating the CCMM server information in Contact Center Manager Administration on page 645
- Updating the HOSTS file on page 570 (CCT) **OR** Joining the server to the domain on page 571

Changing the server name on the operating system

About this task

Change the Contact Center Multimedia 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 Contact Center Multimedia server.
2. Choose **Start** > **Control Panel** > **System**.
3. In the **Computer name, domain, and workgroup settings** section, click **Change settings**.
4. Click the **Computer Name** tab.
5. Click **Change**.
6. Enter the new server name.
7. Click **OK**.
8. 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 CCMM name. See Synchronizing the operating system name with the CCMM name on page 639.
9. If you are using a Domain Name Service, contact your local network prime to update the DNS with the new server name.

Changing the CCMM server name in the Dashboard

Before you begin

- Change the name of the Contact Center Multimedia. See Changing the server name on the operating system on page 638.

About this task

Change the name of the Contact Center Multimedia server in the Dashboard to ensure that the CCMM Web admin launches properly.

Procedure

1. On the Contact Center Multimedia server, select **Start** > **All Programs** > **Avaya** > **Contact Center** > **Multimedia Server** > **Multimedia Dashboard**.
2. On the CCMM Dashboard, under **Server Availability**, right-click **Contact Center Manager Administration** and select **Edit**.
3. On the **Administrator Login** dialog, in the **User Name** box, type `GeneralAdmin`.
4. In the **Password** box, type the password. The default password is "__ccmm!".
5. Click **Login**.
6. On the **Administrator Login** dialog, in the text box, type the name for the current Contact Center Manager Administration server.
7. Click **Save**.

Synchronizing the operating system name with the CCMM name

Before you begin

- Verify the server name change. See Verifying the server name change on page 593.

About this task

Synchronize the operating system name with the Contact Center Multimedia name to ensure that the Contact Center suite uses the new server name.

Procedure

1. Log on to the Contact Center Multimedia as administrator.
2. Close the **System Control and Monitor Utility** if it is running.

3. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **Computer Name Synchronisation 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.

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. Click **Start** > **Run**.
2. Type `cmd`.
3. Click **OK**.
4. In a Command line window, type `ping <server name>`.
5. Verify that the IP address matches the IP address of the server with the new name.

Variable definitions

Name	Description
server name	The name of the Contact Center Multimedia.

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 2008 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 2008 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.

Joining the server to the domain

About this task

If you are using a domain and a DNS, you join the server to the domain. This ensures that all servers can interpret the new server name.

Procedure

1. Log on to the server.
2. Change the server name or IP address.
3. Remove the server from the domain.

4. Join the server back to the domain using the new server name and IP address.

Updating the e-mail attachment folders

Before you begin

- Ensure that you have the e-mail feature installed and enabled using the Contact Center License Manager.

About this task

Update the e-mail attachment folders for Contact Center Multimedia. If you are licensed for e-mail messages in your contact center, you must update the e-mail attachment folders.

Procedure

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, select **E-mail**.
3. Select **General Settings**.
4. In the **Attachment Files** area, update the path to match the new server path.
5. Click **Save**.

Configuring the external Web server

Before you begin

- Know the custom interface folder names and paths for the web.xml and .jsp files for the sample customer Web installation.

About this task

Configure the external Web server to update the files with the new server name if you have an external Web server in your contact center. 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 server.
2. On the **Start** menu, choose **All Programs** > **Administrative Tools** > **Services**.
3. Right-click **Apache Tomcat** service, and click **Stop**.
4. Close the Services window.

5. On the external Web server, navigate to ..\webapps\CI_Sample_Website\WEB-INF.
6. Open the web.xml file in Notepad or another text editor.
7. Locate the text string <param-name>CCMM_HOSTNAME</paramname>.
8. In the <param-name> line, replace the old server name with the name of the new server.
9. Save and close the file.
10. On the external Web server, navigate to ..\webapps\WebComms\WEB-INF.
11. Open the web.xml file in Notepad or another text editor.
12. Locate the text string <param-name>CCMM_HOSTNAME</paramname>.
13. In the <param-name> line, replace the old server name with the new server name.
14. Save and close the file.
15. Delete all files in the following folders:
    - ..\Program Files\Apache Software Foundation\Tomcat 5.5\work\Catalina \localhost\CI_Sample_Website\org\apache\jsp
    - ..\Program Files\Apache Software Foundation\Tomcat 5.5\work\Catalina \localhost\WebComms\org\apache\jsp
16. On the **Start** menu, choose **All Programs** > **Administrative Tools** > **Services**.
17. Right-click **Apache Tomcat** service, and click **Start**.
18. Close the Services window.

Variable definitions

Name	Description
CCMM_HOSTNAME	The name of the Contact Center Multimedia server.

Configuring the external Web server while using Webcom 6.2 (xampp 1.7.3 or higher)

Before you begin

- Know the custom interface folder names and paths for the web.xml and .jsp files for the sample customer Web installation.

About this task

Configure the external Web server to update the files with the new server name if you have an external Web server in your contact center. 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 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.

Configuring the Agent Desktop

Before you begin

- Ensure that agents use the Agent Desktop.
- Change the name of the Contact Center Multimedia server in the operating system. See Changing the server name on the operating system on page 638.
- Uninstall the Agent Desktop. For more information on installing the Agent Desktop, see *Avaya Aura® Contact Center Installation* (NN44400-311).

About this task

Configure the Agent Desktop to allow agents to monitor calls and make calls using the telephony toolbar.

Procedure

Install the Agent Desktop.

Important:

Install Agent Desktop using the new server name.

Variable definitions

Name	Description
URL	The Uniform Resource Locator (URL) agents use to access the Agent Desktop. The format of the URL is http://<servername>/agentdesktop/CCADClickOnce.application.

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 638.

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.
Password	The password used for the ID used to generate multimedia reports. The default user password is mmRep.

CCMM server IP address change

Change the IP address of the Contact Center Multimedia server and update the properties of all of the other servers in the Contact Center Suite.

CCMM server IP address change procedures

About this task

This task flow shows you the sequence of procedures you perform to change the IP address of the Contact Center Multimedia server. To link to any tasks, click on CCMM server IP address change navigation on page 647.

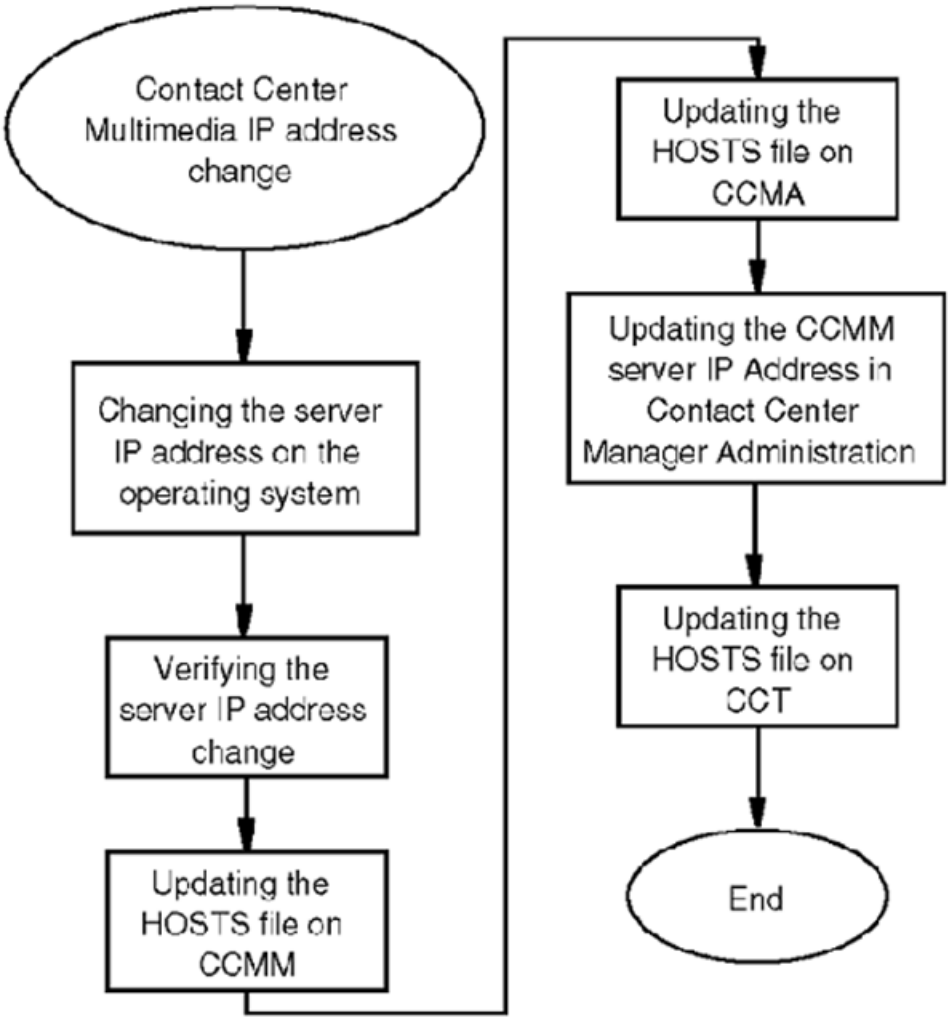


Figure 18: CCMM server IP address change procedures

CCMM server IP address change navigation

- Changing the IP address on the operating system on page 648
- Verifying the server IP address change on page 648
- Updating the HOSTS file on page 570 (CCMM)
- Updating the HOSTS file on page 570 (CCMA)
- Updating the CCMM server IP address in Contact Center Manager Administration on page 650
- Updating the HOSTS file on page 570 (CCT)

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. From the **Start** menu, choose **Control Panel**.
4. Click **Network and Internet** > **Network Sharing Center**.
5. Click **Change adapter settings**.
6. Right-click the LAN connection, and then click **Properties**.
7. Select **Internet Protocol (TCP/IP)**, and then click **Properties**.
8. In the **IP Address** box, type the new IP address.
9. Click **OK**.
10. On the Properties window, click **Close**.
11. 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. Click **Start** > **Run**.
2. Type `cmd`.
3. Click **OK**.
4. In a Command line window, type `ping <server name>`.

5. Verify that the IP address matches the new IP address of the server.

Variable definitions

Name	Description
server name	The name of the Contact Center Multimedia 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 2008 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 2008 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 648.

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.

Appendix B: Default login values

For security purposes, 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–with no Security Framework	webadmin	webadmin	
Administration user for UCM Commissioning–with Security Framework	admin	<configured by user>	
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

access class ... 78, 80, 82
  create ... 78
  delete ... 82
  modify ... 80
access classes ... 77, 79, 252
  add ... 252
  operations ... 77
  view members ... 79
access classes operations ... 77–82
  create access class ... 78
  delete access class ... 82
  logon to Server Utility ... 77
  modify access class ... 80
  preview list of access classes ... 81
  print list of access classes ... 81
  view members of access classes ... 79
access to email message text ... 455
  control ... 455
active callback timer ... 458
  configure ... 458
active callback trunk access ... 458
  configure ... 458
active contact timer ... 457
  configure ... 457
Active Directory user to CCMM ... 408
  import ... 408
active sessions ... 241
  view ... 241
AD-LDS ... 183
  replication ... 183
AD-LDS replication ... 184, 186, 187
  choose AD-LDS service accounts ... 186
  setup ... 184
  setup AD-LDS replication ... 184
  start replication on replicating servers ... 187
  stop replication on replicating servers ... 187
AD-LDS service accounts ... 186
  choose ... 186
add ... 91, 111, 138, 205, 206, 229, 247, 250, 252, 253, 258, 307, 326, 367, 368, 379, 381, 391, 392, 406, 411, 415, 416
  access classes ... 252
  administrators ... 307
  desktop user accounts ... 91
  document imaging server ... 379
  email server ... 326
  event preference ... 111
  expert manually to CCMM ... 406
  experts to a skillset ... 411
  external account (optional) ... 206
  fax mailbox ... 392
  fax server ... 391
  local user identity and password ... 205
  network skillset ... 258
  new Contact Center application ... 229
  scanned document mailbox ... 381
  site ... 247
  site in CCMS ... 253
  site to the NCC ... 250
  SMS Gateway ... 415
  SMS mailbox ... 416
  specified length to all voice segments ... 138
  voice mail mailbox ... 368
  voice mail server ... 367
add a new Contact Center application ... 230
  variable definitions ... 230
add event preference ... 112
  variable definitions ... 112
add external account (optional) ... 207
  variable definitions ... 207
add fax mailbox ... 393
  variable definitions ... 393
add local user identity and password ... 206
  variable definitions ... 206
add scanned document mailbox ... 381
  variable definitions ... 381
add site to the NCC ... 251
  procedure job aid ... 251
add SMS mailbox ... 417
  variable definitions ... 417
add voice mail mailbox ... 369
  variable definitions ... 369
admin password ... 235
  change ... 235
administer ... 83
  connected user and user account operations ... 83
administration ... 249, 272, 447, 515, 519
  console ... 272
  licensing ... 519
  NCC server ... 249
  Predictive Outbound ... 447

SNMP ... 515
administrators ... 307, 308
add ... 307
remove ... 308
agent access to contacts ... 455
configure ... 455
Agent Desktop ... 23, 171, 296, 299, 301, 453
configure ... 453
enable Call Center Elite environment ... 23, 171
process email contacts ... 296, 299
process outbound contacts ... 301
Agent Desktop Advanced Settings ... 467
configure ... 467
Agent Desktop behavior ... 460
Audible Alert ... 460
Bring to front ... 460
configure ... 460
Give focus ... 460
Agent Desktop configuration ... 453–467
change a closed reason ... 462
change custom fields in Agent Desktop ... 456
configure active contact timer ... 457
configure Advanced Settings ... 467
configure agent access to contacts ... 455
configure Agent Desktop behavior ... 460
configure callback timer ... 458
configure callback trunk access ... 458
configure default closed reasons ... 463
configure hotdesking ... 461, 462
Citrix environment ... 462
configure Screen Pops ... 465
configure state of the Agent terminal ... 461
log off ... 461
control access to email message text ... 455
create a closed reason ... 462
create custom fields in Agent Desktop ... 456
delete closed reason ... 464
delete custom field in Agent Desktop ... 456
enable customer history on voice contacts ... 466
prerequisites ... 453
reset agent password ... 454
specify email attachment size ... 459
Agent Desktop Displays parameters on the server ... 158, 159
configure ... 158
variable definitions ... 159
Agent Order Preference ... 261
configure ... 261
agent password ... 454
reset ... 454
agent timers ... 429
configure ... 429
agent-supervisor ... 23
barge-in ... 23
observe ... 23
agent-supervisor barge-in ... 445
configure intrinsics ... 445
agent-supervisor observe ... 445
configure intrinsics ... 445
alarm ... 105
configure ... 105
Alarm Monitor ... 115–118
manually clear an alarm ... 118
obtain more information about alarms ... 117
open ... 115
refresh ... 115
sort events ... 116
Alarm Monitor appears in the foreground ... 117
procedure job aid ... 117
alias for a recipient mailbox ... 331
change ... 331
create ... 331
all silence from all voice segments ... 139
remove ... 139
anonymous Web communcations ... 432
allowing ... 432
application commands ... 33–35
database integration service functionality ... 33
GET RESPONSE ... 34
SEND INFO ... 35
SEND REQUEST ... 34
apply ... 310
office hours ... 310
apply the security template ... 504, 506
locally on the server ... 504
network domain ... 506
archive ... 476–480
closed reason ... 479
email rule ... 477
outbound campaign ... 476
restore ... 480
skillset ... 478
archive utility ... 476
start ... 476
assign ... 427
development Web server name ... 427
assign a development Web server name ... 427
variable definitions ... 427
assign role ... 215
user ... 215
assign user ... 216
role ... 216

authentication scheme 227
create 227
automatic phrases (IM) 403, 404
create 403
delete 404
automatic phrases (Web communications) 433, 434
create 433
delete 434
Avaya CRQM 168
configure 168
Avaya Media Server 485, 564
change name or IP address 564
configuration 485
Avaya Media Server configuration 485
prerequisites 485
Avaya Media Server server 565
rename the name or IP address 565
Avaya Mentor videos 28

B

backup 73, 531
Database Integration Service 73
restore 531
backup location 526
create 526
backup of the database 529
schedule 529
barred email address 357
delete 357
barring 357
outgoing email address 357
bulk resources 285, 286
export 286
import 285

C

capture 178–182
CDN data 180
IVR ACD-DN data 181
route data 182
TN data 178
voice port data 179
capturing terminal data 178
example 178
CCMA 145, 189, 497, 607
configure 145
failure recovery 189
logon warning message 497
server name change 607
CCMA configuration 145–149, 152–154, 156–158, 160, 162, 164, 166–171
change iceAdmin user account password 160
configure Agent Desktop Displays parameters on the server 158
configure Avaya CRQM 168
configure CDN Landing Pads for Integrated Reporting 169
configure CDN Landing Pads for Universal Networking 169
configure Contact Center License Manager service 146
configure DNIS Landing Pads for Universal Networking 170
configure email notifications (Historical reporting) 153
configure Emergency Help 152
configure logon warning message title and text 147
configure LPR port for printers 162
configure network printer on the CCMA server 162
configure network printer to use a print server other than the CCMA server 166
configure network printer to use the CCMA server as the print server 164
configure Real-Time Reporting 149
configure SMTP server 154
create shared folder to export historical reports 156
enable Call Center Elite environment in Agent Desktop 171
enable logon warning message 148
install Orchestration Designer 157
install XML Automated Assignments feature 167
prerequisites 145
CCMA failure recovery 189, 191
job aid 191
prerequisites 189
tasks 189
CCMA security details 198
configure 198
CCMA server IP address 617
change 617
CCMA server IP address change 617–619
change the server IP address on the server 618
tasks 617, 619
CCMA server name change 608, 610–613, 616
change the CCMA server name in the Multimedia Dashboard 616
change the server name in the operating system 610
prerequisites 608
synchronize the operating system name 611
CCMA name 611

tasks ... 608
update historical report output files ... 613
variable definitions ... 612
CCMM ... 291, 305
fundamentals ... 291
general configuration ... 305
CCMM fundamentals ... 292, 295, 297–299, 302, 303
email contact type ... 292
email traffic reports ... 295
fax ... 297
instant Messaging ... 302
mailbox configuration ... 298
office hours ... 303
outbound contact type ... 299
scanned documents ... 297
SMS ... 297
traffic reports ... 298
voice mail ... 297
Web communications ... 302
CCMM general configuration ... 305–316, 319
add administrators ... 307
apply office hours ... 310
configure displayed date for traffic reports ... 311
configure geographic alternate CCT server ... 315
configure holidays ... 309
configure LDAP server ... 316
configure office hours ... 308
configure Predictive server ... 319
configure reporting credentials ... 306
configure system license ... 306
configure Web communications comfort groups 314
WC skillset ... 314
configure Web On Hold comfort groups ... 312
WC skillset ... 312
delete geographic alternate CCT server ... 316
prerequisites ... 305
remove administrators ... 308
remove Web communications comfort groups ... 314
WC skillset ... 314
remove Web On Hold comfort groups ... 313
WC skillset ... 313
view ... 311
real-time traffic reports by contact ... 311
CCMM server IP address ... 646
change ... 646
CCMM server IP address change ... 646, 648, 650
change the IP address on the operating system 648
tasks ... 646
update the CCMM server IP address in CCMA . 650
verify the server IP address change ... 648
CCMM server name ... 635
change ... 635
CCMM server name change 636, 638–640, 642, 644, 645
change the server name on the operating system 638
configure Agent Desktop ... 644
configure the external Web server ... 642, 644
Webcom 6.2 ... 644
prerequisites ... 636
synchronize the operating system name ... 639
CCMM name ... 639
tasks ... 636
update CCMM server information in CCMA ... 645
update email attachment folders ... 642
variable definitions ... 640
CCMM_Security_Policy.msi ... 497
CCMS 31, 32, 37–39, 41, 43, 44, 47, 48, 50, 101, 565, 574
configuration ... 41
CS 1000 PABX data ... 47
database integration service functionality ... 32
feature report ... 37
IP address change ... 574
licensed features configuration ... 44
local settings configuration ... 43
Multicast Address and Port Configuration ... 38
Multicast Stream Control ... 38
Nbconfig ... 31
real-time statistics ... 38
manual ... 38
server configuration ... 38
server name change ... 565
server settings ... 101
SIP Local Subscriber data ... 48
SIP Network Settings data ... 50
web services ... 39
CCMS configuration ... 41
prerequisites ... 41
CCMS Configuration utility ... 42
administration access level ... 42
regular access level ... 42
CCMS connected user operations ... 83
prerequisites ... 83
CCMS IP address change ... 574, 576, 577, 579–582
change Contact Center License Manager IP address ... 580
change ELAN subnet IP address ... 582
change the contact center subnet IP address ... 576
configure CCMS ... 577
tasks ... 574
update CCT license ... 581
update the server IP address in CCMA ... 579
verify IP address change ... 577
CCMS script ... 72

configure ... 72
CCMS Serial port ... 97
configure ... 97
prerequisites ... 97
CCMS server name change ... 566, 568–572, 574, 591
change the server name on the operating system 568
configure Contact Management Framework settings ... 572
prerequisites ... 566
rerun the system configuration ... 574
server name in CCMA ... 571, 591
tasks ... 566
variable definitions ... 570
verify the server name change ... 569
CCMS server settings ... 101
prerequisites ... 101
view server resources ... 101
CCMS statistics ... 55
configuration ... 55
CCMS statistics configuration ... 55–58
change IP multicast settings ... 57
configure Multicast controller ... 56
disconnect Terminal Services sessions ... 58
prerequisites ... 55
CCMS Utility ... 77, 498
access classes operations ... 77
prerequisites ... 77
view CCMS events ... 498
CCT ... 271–274
fundamentals ... 271
Open Interfaces ... 273
Reference Client ... 274
Web Administration ... 272
CCT deployment type ... 277
configure ... 277
CCT fundamentals ... 271–274
ACD ... 271
administration console ... 272
application programming interfaces ... 273
CCT Reference Client ... 274
CCT Web Administration ... 272
programming interfaces ... 272
Trace Control Utility ... 272
Web services ... 273
CCT licensing ... 275
configure ... 275
CCT licensing configure ... 276
variable definitions ... 276
CCT server ... 275
configure ... 275
CCT server configuration ... 275, 277
CCT deployment type ... 277
CCT licensing ... 275
CCT server IP address ... 631
change ... 631
CCT server IP address change ... 631, 633, 635
change the server IP address on the operating system ... 633
tasks ... 631
update the CCT server IP address in CCMA ... 635
verify the server IP address change ... 633
CCT server name ... 623
change ... 623
CCT server name change ... 623, 625–630
change the server name on the operating system 625
configure Agent Desktop ... 630
configure CCMS ... 629
prerequisites ... 623
synchronize the operating system name ... 626
CCT name ... 626
tasks ... 623
update the CCT server name in CCMA ... 628
variable definitions ... 627
CDN data ... 180
capture ... 180
CDN Landing Pads for Integrated Reporting ... 169
configure ... 169
CDN Landing Pads for Universal Networking ... 169
configure ... 169
change .. 43, 44, 47, 48, 50, 57, 94, 110, 113, 114, 125, 160, 235, 246, 329, 331, 337, 340, 345, 347, 352, 355, 437, 440, 443, 456, 462, 521, 523, 563, 565, 574, 582, 598, 617, 623, 631, 635, 646
admin password ... 235
alias for a recipient mailbox ... 331
CCMA server IP address ... 617
CCMM server IP address ... 646
CCMM server name ... 635
CCMS IP address ... 574
CCMS server name ... 565
CCT server IP address ... 631
CCT server name ... 623
character encoding for outgoing email ... 355
closed reason ... 462
co-resident server IP address ... 598
co-resident server name ... 582
CS 1000 PABX data ... 47
custom fields in Agent Desktop ... 456
event classification ... 114
event preference ... 113
filtering criteria for events ... 110
iceAdmin user account password ... 160

IP address 563
IP multicast settings 57
keyword group 337
license manager file on CCMS 523
licensed features configuration 44
local settings configuration 43
Nodal to Corporate licensing 521
prepared responses 340
properties of desktop users 94
recipient mailbox 329
rule groups 352
rules 347
sender group 345
sequence of messages 440, 443
Web communications comfort groups 443
Web On Hold comfort groups 440
sequence of URLs 437
Web On Hold URLs groups 437
server name 563
SIP Local Subscriber data 48
SIP Network Settings data 50
site to monitor 125, 246
change admin password 236
variable definitions 236
change CS 1000 PABX data 47
variable definitions 47
change IP multicast settings 58
procedure job aid 58
variable definitions 58
change licensed features configuration 45
variable definitions 45
change local settings configuration 43
variable definitions 43
change name or IP address 564
Avaya Media Server 564
change SIP Local Subscriber data 49
variable definitions 49
change SIP Network Settings data 51
variable definitions 51
change the CCMM server name 592, 593, 639
Administration tool 593
CCMA 593
Dashboard 592, 639
change the CCT server name 591
Administration tool 591
CCMA 591
character encoding 294
outgoing email messages 294
choose 186
AD-LDS service accounts 186
choose AD-LDS service accounts 185
procedure job aid 185
client browsers and shared folders 594, 605, 614, 621
update 594, 605, 614, 621
close 246
Service Monitor 246
closed reason 462, 464, 479
archive 479
change 462
create 462
delete 464
co-resident server IP address 598
change 598
co-resident server IP address change 598, 600, 601, 603, 606, 607
change contact center subnet IP address 600
configure the co-resident server IP address 601
tasks 598
update CCMM server IP address in CCMA 607
update CCT server IP in CCMA 606
update CCT server provider IP address 606
update the server IP address in CCMA 603
verify the server IP address change 601
co-resident server name 582
change 582
co-resident server name change 583, 586, 588, 590, 596
change the server name 586
operating system 586
configure destination for exported scheduled reports 590
configure the Contact Management Framework 596
prerequisites 583
tasks 583
variable definitions 588
compatibility 194
language family 194
configure 24, 41, 55, 56, 61, 63, 64, 67, 68, 72, 97, 103, 105, 119, 121, 123, 126, 127, 145–147, 149, 152–154, 158, 162, 164, 166, 168–170, 197, 198, 201, 221, 245, 255, 260–262, 264–266, 275, 277, 298, 306, 308, 309, 311, 312, 314–316, 319, 321, 323, 325, 328, 353, 358, 365, 366, 377, 378, 383, 389, 390, 395, 401, 402, 413, 414, 419, 425, 428, 429, 431, 448, 450, 451, 453, 455, 457, 458, 460–463, 465, 467, 471, 518, 534, 539, 541, 542, 544, 547, 549, 551, 572, 596, 642, 644
active callback timer 458
active callback trunk access 458
active contact timer 457
agent access to contacts 455
Agent Desktop 453
Agent Desktop Advanced Settings 467

Agent Desktop behavior 460
Agent Desktop Displays parameters on the server 158
Agent Order Preference 261
agent timers 429
alarm 105
Avaya CRQM 168
CCMA 145
CCMA security details 198
CCMS 41
CCMS script 72
CCMS statistics 55
CCT deployment type 277
CCT licensing 275
CCT server 275
CDN Landing Pads for Integrated Reporting 169
CDN Landing Pads for Universal Networking 169
Contact Center License Manager service 146
Contact Management Framework 596
Contact Management Framework settings 572
CS 100 PABX 103
customer notification log 431
database connections 67
Database Integration Wizard 61
default closed reasons 463
default site information 126
disconnect messages 402
displayed date for traffic reports 311
DNIS Landing Pads for Universal Networking 170
DNIS network CDNs 266
email 323
email notifications (Historical reporting) 153
email server names 325
email settings 353
Emergency Help 152
event 105
external identity repository 221
external Web server 642, 644
Webcom 6.2 644
fax 389
fax reply mailbox 395
geographic alternate CCT server 315
HDX server settings 64
historical statistics collection 264
holidays 309
hotdesking 461, 462
Citrix environment 462
instant message 401
Integrated Reporting 534
LDAP server 316
logon warning message title and text 147
LPR port for printers 162
mailbox 298
MCDN network CDNs 265
Microsoft Exchange for sending outgoing email 358
Mission Critical High Availability on the active server 549
Mission Critical High Availability on the standby server 551
mmReport user 306
Multicast controller 56
Multimedia server settings 572, 596
network communication parameters 255
network printer on the CCMA server 162
network printer to use a print server other than the CCMA server 166
network printer to use the CCMA server as the print server 164
network skillset properties 260
NMS 518
notification of automatic switchovers 542
office hours 308
outbound 321
PC Event Browser 121
Phonebook LDAP server 24
predictive blending settings 448
predictive outbound 451
agent scripts 451
Predictive server 319
Provider 119
Real-Time Reporting 149
reporting credentials 306
route point 378, 390
fax skillset 390
scanned document skillset 378
route point for a voice mail skillset 366
route point for an SMS skillset 414
routing table assignments 262
routing tables 261
RTD Multicast settings 450
scanned document 377
scanned document reply mailbox 383
Screen Pops 24, 465
Security Framework 197
security prompts in Internet Explorer 201
Serial port 97
Service Monitor 123, 245
service monitoring 544
skillsets for email 328
SMS 413
SMS reply mailbox 419
SMTP server on CCMA server 154

state of the Agent terminal 461
log off 461
system data source names 63
system license 306
TAPI server settings 64
user 471
voice mail 365
Voice Prompt Editor 127
warm standby or hot-standby automatic switchovers 547
warm standby or hot-standby managed IP address 539
warm standby or hot-standby manual switchovers 544
warm standby or hot-standby server 541
Web communications 425
Web communications comfort groups 314
WC skillset 314
Web On Hold comfort groups 312
WC skillset 312
Web services 68
welcome messages 402, 428
configure Agent Desktop 645
variable definitions 645
configure Agent Desktop Advanced Settings 467
variable definitions 467
configure Agent Desktop behavior 460
variable definitions 460
configure CCMA security details 198
variable definitions 198
configure CCT deployment type 278
variable definitions 278
configure contact timers 430
variable definitions 430
configure email server names 326
variable definitions 326
configure Event Browser 105
prerequisites 105
configure fax reply mailbox 396
variable definitions 396
configure HDX and TAPI server settings 66
procedure job aid 66
configure Integrated Reporting 535
variable definitions 535
configure intrinsics 445
agent-supervisor barge-in 445
agent-supervisor observe 445
configure Mission Critical High Availability on the active server 550
variable definitions 550
configure Mission Critical High Availability on the standby server 552
variable definitions 552
configure notification of automatic switchovers 543
variable definitions 543
configure operating system for remote access ..511, 512
domain 511
workgroup 512
configure predictive blending settings 450
variable definitions 450
configure route point 321
Outbound skillset 321
configure route point for a fax skillset 390
variable definitions 390
configure route point for a scanned document skillset 378
variable definitions 378
configure route point for a voice mail skillset 366
variable definitions 366
configure route point for an Outbound skillset 322
variable definitions 322
configure scanned document reply mailbox 384
variable definitions 384
configure service monitoring 546
variable definitions 546
configure SMS reply mailbox 420
variable definitions 420
configure SMTP server on CCMA server 156
variable definitions 156
configure warm standby or hot-standby managed IP address 540
variable definitions 540
configure warm standby or hot-standby server 542
variable definitions 542
configure Web communications ..426–429, 431, 433–440, 442–445
assign a development Web server name 427
change sequence of messages 440, 443
Web communications comfort group 443
Web On Hold comfort group 440
change sequence of URLs 437
Web On Hold URLs group 437
configure agent timers 429
configure customer notification log 431
configure intrinsics 445
agent-supervisor barge-in 445
agent-supervisor observe 445
configure text chat labels 428
configure welcome messages 428
create automatic phrases (Web communications) 433
create page push URL (Web communications) . 434

create Web communications comfort groups 442
create Web On Hold comfort groups 439
create Web On Hold URLs groups 436
delete automatic phrases (Web communications) 434
delete message 440, 444
Web communications comfort group 444
Web On Hold comfort group 440
delete page push URL (Web communications) ..435
delete URL 437
Web On Hold URL group 437
delete Web communications comfort group 444
delete Web On Hold URLs group 438
prerequisites 426
configure welcome messages and text chat labels .. 429
variable definitions 429
configuring 254
Landing Pads 254
console 272
administration 272
construct and test 70
SQL statements 70
stored procedures 70
construct and test SQL statements or stored procedure 71
procedure job aid 71
contact center 303
office hours 303
Contact Center applications 559
start 559
stop 559
Contact Center database 525
maintenance 525
Contact Center database maintenance 525–527, 529, 531, 533, 534
configure 534
create backup location 526
migrate the database 533
perform immediate backup of the database 527
prerequisites 525
recover a scheduled backup 531
restore a backup 531
schedule backup of the database 529
Contact Center License Manager service 146
configure 146
Contact Center server 537
High Availability 537
Contact Center server High Availability 538, 539, 541, 542, 544, 547–549, 551, 553, 554
configure Mission Critical High Availability on the active server 549
configure Mission Critical High Availability on the standby server 551
configure notification of automatic switchovers ..542
configure service monitoring 544
configure warm standby or hot-standby automatic switchovers 547
configure warm standby or hot-standby managed IP address 539
configure warm standby or hot-standby manual switchovers 544
configure warm standby or hot-standby server ..541
monitor switchover information 547
prerequisites 538
review shadowing 548
start a Mission Critical Active Server 553
start shadowing on a Mission Critical Standby Server 553
stop High Availability on a Mission Critical active server 554
stop High Availability on a Mission Critical standby server 554
Contact Center server High redundancy 538
prerequisites 538
Contact Management Framework 596
configure 596
Contact Management Framework settings 572
configure 572
contact types 292, 299
email 292
outbound 299
control 455
access to email message text 455
copy 131
voice file 131
copy from another role 212
mapping elements and permissions 212
create ... 36, 62, 78, 129, 132, 156, 209, 217, 227, 329, 331, 337, 340, 345, 347, 352, 403, 404, 409, 433, 434, 436, 439, 442, 456, 462, 526
access class 78
alias for a recipient mailbox 331
authentication scheme 227
automatic phrases (IM) 403
automatic phrases (Web communications) 433
backup location 526
closed reason 462
custom fields in Agent Desktop 456
custom role 209
expert group 409
keyword group 337
page push URL 404

page push URL (Web communications) 434
policy 217
prepared responses 340
recipient mailbox 329
role 209
rule groups 352
rules 347
security policy for passwords 217
sender group 345
shared folder to export historical reports 156
stored procedure 62
stored procedures 36
voice file 129
voice segment 132
Web communications comfort groups 442
Web On Hold comfort groups 439
Web On Hold URLs groups 436
create and invoke stored procedure 62
example 62
create backup location 526
variable definitions 526
create custom role 210
variable definitions 210
create expert group 410
variable definitions 410
create or change a keyword group 338
variable definitions 338
create or change an alias for a recipient mailbox 332
variable definitions 332
create or change prepared responses 342, 343
procedure job aid 343
variable definitions 342
create or change recipient mailbox 330
variable definitions 330
create or change rule groups 353
variable definitions 353
create or change rules 349
variable definitions 349
create or change sender group 346
variable definitions 346
CS 100 PABX 103
configure 103
CS 100 PABX configuration 103
prerequisites 103
CS 1000 173
Data Extraction Tool operation 173
CS 1000 Data Extraction Tool operation 173–175, 177–182
capture CDN data 180
capture IVR ACD-DN data 181
capture route data 182
capture TN data 178
capture voice port data 179
extract data 174, 175, 177
file 177
modem 175
serial connection 174
prerequisites 173
CS1000 data 281
import 281
custom field in Agent Desktop 456
delete 456
custom fields in Agent Desktop 456
change 456
create 456
custom role 209
create 209
custom role (optional) 210
delete 210
customer history on voice contacts 466
enable 466
customer notification log 431
configure 431

D

data 475
collection 475
management 475
data collection and management 475–481
archive by closed reason 479
archive by email rule 477
archive by skillset 478
archive outbound campaign 476
prerequisites 475
recover from a failed archive or restore 481
restore an archive 480
start the archive utility 476
database 533
migrate 533
database connections 67
configure 67
Database Integration Service 73
backup 73
database integration service functionality 32, 33, 36
application commands 33
HDX 32
stored procedures 36
Database Integration Wizard 61
configure 61
Database Integration Wizard configuration 61–64, 67–74
backup Database Integration Service 73

configure CCMS script ... 72
configure database connections ... 67
configure HDX and TAPI server settings ... 64
configure system data source names ... 63
configure Web services ... 68
construct and test SQL statements or stored procedure ... 70
create and invoke stored procedure ... 62
delete SQL statements or stored procedure ... 72
prerequisites ... 61
remove Web service package ... 69
restore ... 74
update SQL statements ... 71
date and time features ... 509
manage ... 509
default ... 651
login values ... 651
default closed reasons ... 463
configure ... 463
default site information ... 126
configure ... 126
default site information (client machine) ... 247
set ... 247
delete ... 72, 82, 95, 114, 131, 140, 210, 231, 238, 259, 316, 327, 333, 339, 340, 343, 346, 351, 357, 368, 371, 380, 383, 385, 392, 395, 397, 404, 405, 410, 411, 416, 419, 421, 434, 435, 438, 444, 456, 464
access class ... 82
automatic phrases (IM) ... 404
automatic phrases (Web communications) ... 434
barred email address ... 357
closed reason ... 464
custom field in Agent Desktop ... 456
custom role (optional) ... 210
desktop user accounts ... 95
document imaging server ... 380
email server ... 327
event preference ... 114
expert group ... 410
experts from a skillset ... 411
fax mailbox ... 395
fax reply mailbox ... 397
fax server ... 392
geographic alternate CCT server ... 316
keyword from a keyword group ... 339
keyword group ... 340
network skillset ... 259
page push URL ... 405
page push URL (Web communications) ... 435
prepared responses ... 343
recipient mailbox ... 333
rules ... 351
scanned document mailbox ... 383
scanned document reply mailbox ... 385
secured element ... 231
sender group ... 346
SMS Gateway ... 416
SMS mailbox ... 419
SMS reply mailbox ... 421
SQL statements ... 72
stored procedures ... 72
user account ... 238
voice file ... 131
voice mail mailbox ... 371
voice mail server ... 368
voice segment ... 140
Web communications comfort group ... 444
Web On Hold URL group ... 438
delete message ... 440, 444
Web communications comfort group ... 444
Web On Hold comfort group ... 440
delete sender ... 347
sender group ... 347
delete URL ... 437
Web On Hold URL group ... 437
deleting a site ... 251
NCC ... 251
desktop password ... 93
reset ... 93
desktop user accounts ... 91, 95
add ... 91
delete ... 95
determine ... 362
SMTP Authentication is enabled ... 362
disable ... 199, 237, 351, 510, 561
rules ... 351
Security Framework ... 199
services ... 561
user account ... 237
Windows time service ... 510
disable Auto Startup ... 555
Mission Critical HA ... 555
disconnect ... 58
Terminal Services sessions ... 58
disconnect messages ... 402
configure ... 402
displayed date for traffic reports ... 311
configure ... 311
DNIS Landing Pads for Universal Networking ... 170
configure ... 170
DNIS network CDNs ... 266
configure ... 266

document imaging server 379, 380
add 379
delete 380
update 379
download and inspect 233
security log 233

E

edit 98, 230
port settings 98
secured element 230
element 229
management 229
Element 211
mapping 211
element management 229–231
add a new Contact Center application 229
delete a secured element 231
edit a secured element 230
elements from a role 213
removal 213
email 293, 323
configure 323
rule groups 293
email attachment folders 642
update 642
email attachment size 459
specify 459
email configuration 324–329, 331, 333, 334, 336, 337, 339, 340, 343–347, 350–353, 355–359, 361, 362
add email server 326
barring email address 357
change character encoding 355
outgoing email 355
configure email server names 325
configure email settings 353
configure Microsoft Exchange for sending outgoing email 358
configure skillsets 328
email 328
create or change a keyword group 337
create or change a sender group 345
create or change an alias for a recipient mailbox 331
create or change prepared responses 340
create or change recipient mailbox 329
create or change rule groups 352
create or change rules 347
delete a barred email address 357
delete a keyword from a keyword group 339
delete a keyword group 340
delete a recipient mailbox 333
delete a rule 351
delete a sender group 346
delete email server 327
delete prepared responses 343
delete sender from a sender group 347
determine if SMTP Authentication is enabled 362
disable a rule 351
enable a rule 350
prerequisites 324
promote suggested responses 344
remove attachments from prepared responses . 344
select outgoing email address 356
SMTP Authentication 361
email server 361
SSL 359
Email Manager 359
update the system default rule 334
update the system delivery failure rule 336
email contact type 293–295
character encoding 294
outgoing email messages 294
email rule groups 293
inbound email settings 294
Internationalized domain names 295
outbound email settings 294
recipient mailbox 293
email contact types 296, 297
CCMA 296
Web services 297
email notifications (Historical reporting) 153, 154
configure 153
variable definitions 154
email rule 477
archive 477
email server 326, 327, 361
add 326
delete 327
SMTP authentication 361
email server names 325
configure 325
email setting 355
configure 355
email settings 353
configure 353
email traffic 295
reports 295
Emergency Help 152
configure 152
enable 23, 24, 148, 350, 432, 466, 561
Call Center Elite in Agent Desktop 23
customer history on voice contacts 466

Customer History on Voice Contacts 24
logon warning message 148
rules 350
services 561
Web Communications transfer to a skillset 23
Web Communications transfer to skillset 432
enable Call Center Elite environment 171
Agent Desktop 171
end 241
sessions manually 241
event 105
configure 105
Event Browser 106–111, 113, 114
add event preference 111
change event classification 114
change event preference 113
change filtering criteria for events 110
delete event preference 114
print a list of events 109
print list of event preference 113
save a list of events 109
sort events 108
start 106, 107
Server Utility 107
view online Help for an event 108
Event Browser and Alarm Monitor 105
event classification 114
change 114
event preference 111, 113, 114
add 111
change 113
delete 114
Event severity 496
Critical 496
Information 496
Major 496
Minor 496
Event viewer 495
settings 495
events 112
throttle 112
example 62, 178, 180, 181
capturing terminal data 178
create and invoke stored procedure 62
option 11C for IVR ACD-DNs output 181
Overlay program 23 output 181
Overlay program 81 output 180
exit 125
Networking Service Monitor 125
expert from files to CCMM 406
import 406
expert group 409, 410
create 409
delete 410
expert manually to CCMM 406
add 406
experts from a skillset 411
delete 411
experts to a skillset 411
add 411
export 286
bulk resources 286
external account (optional) 206
add 206
external identity repository 221
configure 221
external identity repository configuration 221, 223–225, 227
create authentication scheme 227
provision Kerberos external authentication server 225
provision LDAP external authentication server 223
provision RADIUS external authentication server 224
tasks 221
external Web server 642
configure 642
extract data 174, 175, 177
file 177
modem 175
serial connection 174

F

failure recovery 189
CCMA 189
fax 389
configure 389
fax configuration 389–392, 394, 395, 397, 398
add fax mailbox 392
add fax server 391
configure fax reply mailbox 395
configure route point 390
fax skillset 390
delete fax mailbox 395
delete fax reply mailbox 397
delete fax server 392
prerequisites 389
update fax 397, 398
system default rule 397
system delivery failure rule 398
update fax mailbox 394
update fax server 391
fax mailbox 392, 394, 395

add ... 392
delete ... 395
update ... 394
fax reply mailbox ... 395, 397
configure ... 395
delete ... 397
fax server ... 391, 392
add ... 391
delete ... 392
update ... 391
fax system default rule ... 397
update ... 397
fax system delivery failure rule ... 398
update ... 398
features ... 19, 21–24, 38
agent-supervisor observe and barge-in ... 23
Customer History on Voice Contacts ... 24
enable Call Center Elite ... 23
geographic alternate CCT server ... 24
High Availability ... 19
inline attachments ... 22
Licensing ... 22
Phonebook LDAP server ... 24
Real-Time Statistics Multicast (RSM) ... 38
Screen Pops ... 24
SIP-enabled contact center ... 21
Web communications comfort groups ... 22
Web Communications transfer to a skillset ... 23
Web On Hold comfort groups ... 22
file ... 177
extract data ... 177
filtering criteria for events ... 110
change ... 110
fundamentals ... 193, 271, 291, 495
CCMM ... 291
CCT ... 271
language support ... 193
security ... 495

G

geographic alternate CCT server ... 315, 316
configure ... 315
delete ... 316
grace period ... 520
reset ... 520
group of voice segments ... 135
play ... 135

H

HDX ... 32
database integration service functionality ... 32
HDX and TAPI server settings ... 64
configure ... 64
high availability ... 556
reinstate ... 556
High Availability ... 537
High Availability on a Mission Critical active server ... 554
stop ... 554
High Availability on a Mission Critical standby server 554
stop ... 554
High Availability solution server ... 563
renaming considerations ... 563
Historical Reporting (email contacts) ... 296
outbound contacts ... 296
Historical Reporting (outbound contacts) ... 301
outbound contacts ... 301
historical statistics collection ... 264
configure ... 264
holidays ... 309
configure ... 309
HOSTS file 570, 579, 588, 603, 615, 622, 627, 634, 641, 649
update 570, 579, 588, 603, 615, 622, 627, 634, 641, 649
HOSTS file for clients ... 594, 604, 613, 620
update ... 594, 604, 613, 620
hotdesking ... 461
configure ... 461

I

iceAdmin password ... 589, 612
reset ... 589, 612
iceAdmin user account password ... 160
change ... 160
immediate backup of the database ... 527
perform ... 527
import ... 200, 280, 281, 284, 285, 406, 408
Active Directory user to CCMM ... 408
bulk resources ... 285
CS1000 data ... 281
expert from files to CCMM ... 406
root certificate authority to Internet Explorer ... 200
Windows users ... 280
workstations from the domain ... 284
import Windows users ... 281
variable definitions ... 281
import workstations from the domain ... 285
variable definitions ... 285
inbound email ... 294
settings ... 294
individual services ... 560
start ... 560

stop ... 560
inline attachments ... 22
auto responses ... 22
auto suggestions ... 22
inspect ... 233
security log ... 233
install ... 157, 167, 515
Orchestration Designer ... 157
Windows SNMP Service ... 515
XML Automated Assignments feature ... 167
instant message ... 401
configure ... 401
instant message configuration ... 401–411
add an expert manually to CCMM ... 406
add experts to a skillset ... 411
configure disconnect messages ... 402
configure welcome messages ... 402
create automatic phrases ... 403
create expert group ... 409
create page push URL ... 404
delete automatic phrases ... 404
delete expert group ... 410
delete experts from a skillset ... 411
delete page push URL ... 405
import an Active Directory user to CCMM ... 408
import an expert from files to CCMM ... 406
prerequisites ... 401
search for users in Active Directory ... 407
Integrated Reporting ... 534
configure ... 534
Internationalized domain names ... 295
East Asian languages ... 295
invoke ... 62
stored procedure ... 62
IP address ... 563
change ... 563
IVR ACD-DN data ... 181
capture ... 181

J

job aid ... 191
CCMA failure recovery ... 191
join the server ... 571, 589, 616, 628, 641
domain ... 571, 589, 616, 628, 641

K

keyword from a keyword group ... 339
delete ... 339
keyword group ... 337, 340
change ... 337
create ... 337
delete ... 340

L

Landing Pads ... 254
configuring ... 254
language ... 194
levels ... 194
language family ... 194
compatibility ... 194
language support ... 193
fundamentals ... 193
language support fundamentals ... 194
language family compatibility ... 194
language levels ... 194
LDAP server ... 316
configure ... 316
length to all voice segments ... 138
add ... 138
remove ... 138
lengthen ... 137
voice segment ... 137
license file ... 521
update ... 521
license manager file on CCMS ... 523
change ... 523
licensing ... 519
administration ... 519
licensing administration ... 520, 521, 523, 524
change Nodal to Corporate licensing ... 521
change the license manager file on CCMS ... 523
refresh servers ... 524
reset grace period ... 520
update license file ... 521
list of access classes ... 81
preview ... 81
print ... 81
list of connected users ... 84
print ... 84
view ... 84
list of event preference ... 113
print ... 113
list of users ... 95
print ... 95
local user identity and password ... 205
add ... 205
log off ... 85, 129
users ... 85
Voice Prompt Editor ... 129
log on ... 77, 128

Server Utility 77
Voice Prompt Editor 128
login values 651
default 651
logon warning message 148, 497
CCMA 497
enable 148
UCM 497
logon warning message title and text 147
configure 147
LPR port for printers 162
configure 162

M

mailbox 293, 298
configuration 298
recipient 293
maintenance 525
Contact Center database 525
manage 209, 217, 233, 235, 241, 279, 509
date and time features 509
policy 217
resource bulk 279
role 209
security log 233
session 241
user accounts 235
user passwords 235
manage user accounts and passwords 235–238
change admin password 235
delete a user account 238
disable a user account 237
reenable a user account 238
reset user password 236
management 229
element 229
manually clear an alarm 118
Alarm Monitor 118
map 215
roles 215
mapping 211
element 211
permission 211
mapping elements and permissions 211, 212
copy from another role 212
role 211
mapping elements and permissions to a role 212
variable definitions 212
MCDN network CDNs 265
configure 265
Microsoft Exchange for sending outgoing email 358
configure 358
Microsoft Windows 509
configure and manage settings 509
Microsoft Windows configuration and management 509–512
configure operating system for remote access .. 511, 512
domain 511
workgroup 512
disable the Windows time service 510
manage date and time features 509
verify Service Packs 511
migrate 533
database 533
migrate the database 534
procedure job aid 534
variable definitions 534
Mission Critical Active Server 553
start 553
Mission Critical HA 555
disable Auto Startup 555
standby auto startup mode 555
Mission Critical High Availability on the active server 549
configure 549
Mission Critical High Availability on the standby server 551
configure 551
modem 175
extract data 175
modify 80
access class 80
monitor 547
switchover information 547
monitor switchover information 548
procedure job aid 548
variable definitions 548
Multimedia server settings 572, 596
configure 572, 596

N

NCC 251
deleting a site 251
NCC server 249, 578, 602
administration 249
update 578, 602
NCC server administration .. 249, 250, 252, 253, 255, 257, 258, 260–262, 264–266
add access classes 252
add network skillset 258
add site in CCMA 253

add site to the NCC 250
configure Agent Order Preference 261
configure DNIS network CDNs 266
configure historical statistics collection 264
configure MCDN network CDNs 265
configure network communication parameters .. 255
configure network skillset properties 260
configure routing table assignments 262
configure routing tables 261
prerequisites 249
synchronize site information 257
network communication parameters 255
configure 255
network printer on the CCMA server 162, 164
configure 162
variable definitions 164
network printer to use a print server other than the CCMA server 166
configure 166
network printer to use the CCMA server as the print server 164
configure 164
network skillset 258, 259
add 258
delete 259
network skillset properties 260
configure 260
Networking Service Monitor 125
exit 125
new Contact Center application 229
add 229
NMS 518
configure 518
Nodal to Corporate licensing 521
change 521
notification of automatic switchovers 542
configure 542

O

obtain more information about alarms 117
Alarm Monitor 117
office hours 308, 310
apply 310
configure 308
online Help for an event 108
view 108
open 115, 130
Alarm Monitor 115
voice file 130
Open Networking Open Interface 39
operation 173
Data Extraction Tool 173
operation 173
operations 77
access classes 77
option 11C for IVR ACD-DNs output 181
example 181
Orchestration Designer 157, 158
install 157
procedure job aid 158
outbound 321
configure 321
outbound campaign 476
archive 476
outbound campaigns 300–302
Campaign Scheduler 301
Outbound Campaign Management Tool 300
Outbound Open Interface 302
outbound configuration 321
configure route point 321
Outbound skillset 321
prerequisites 321
outbound contact type 300, 301
Campaign Scheduler 301
Outbound Campaign Management Tool 300
outbound contact types 301, 302
CCMA 301
Web services 302
outbound email 294
settings 294
Outbound Open Interface 297, 302
outbound campaigns 302
process email contact types 297
Outbound skillset 321
configure route point 321
outgoing email address 356, 357
barring 357
select 356
outgoing email messages 294
character encoding 294
Overlay program 23 output 181
example 181
Overlay program 81 output 180
example 180

P

PABX 103
record information 103
page 471
User Settings 471
page push URL 404, 405

create ... 404
delete ... 405
page push URL (Web communications) ... 434, 435
create ... 434
delete ... 435
PC Event Browser ... 121
start ... 121
PC Event Browser configuration ... 121
prerequisites ... 121
start PC Event Browser ... 121
perform ... 527
immediate backup of the database ... 527
perform immediate backup of the database ... 528
variable definitions ... 528
permission ... 211
mapping ... 211
Platform Security ... 499
securing the server ... 499
play ... 134, 135
a group of voice segments ... 135
voice segment ... 134
policy ... 217
create ... 217
manage ... 217
port settings ... 98
edit ... 98
print ... 98
predictive blending settings ... 448
configure ... 448
predictive outbound ... 451
agent scripts ... 451
configure ... 451
Predictive Outbound ... 447
administration ... 447
Predictive Outbound administration ... 447, 448, 450, 451
configure predictive blending settings ... 448
configure predictive outbound ... 451
agent scripts ... 451
configure RTD Multicast settings ... 450
prerequisites ... 447
Predictive server ... 319
configure ... 319
prepared responses ... 340, 343, 344
change ... 340
create ... 340
delete ... 343
remove attachments ... 344
prerequisites ... 485
Avaya Media Server configuration ... 485
prevent ... 92
users from accessing the server ... 92
preview ... 81
list of access classes ... 81
preview list of access classes ... 81
variable definitions ... 81
print ... 81, 84, 95, 98, 113
list of access classes ... 81
list of connected users ... 84
list of event preference ... 113
list of users ... 95
port settings ... 98
print a list of events ... 109
Event Browser ... 109
procedure job aid .. 58, 66, 71, 86, 106, 117, 151, 158, 185, 186, 251, 343, 533, 534, 548
Alarm Monitor appears in the foreground ... 117
change IP multicast setting ... 58
choose AD-LDS service accounts ... 185
configure HDX and TAPI server settings ... 66
construct and test SQL statements or stored procedure ... 71
create or change prepared responses ... 343
migrate the database ... 534
monitor switchover information ... 548
Orchestration Designer ... 158
Real-Time Reporting ... 151
restore a backup ... 533
set privileges for users ... 86
setup AD-LDS replication ... 186
site to the NCC ... 251
start Event Browser ... 106
process email contacts ... 296, 299
Agent Desktop ... 296, 299
process outbound contacts ... 301
Agent Desktop ... 301
promote ... 344
suggested responses ... 344
properties of desktop users ... 94
change ... 94
Provider ... 119
configure ... 119
start ... 119
Provider configuration ... 119, 120
connect to CCMS ... 120
starting the Provider ... 119
provision ... 205, 223–225
Kerberos external authentication server ... 225
LDAP external authentication server ... 223
RADIUS external authentication server ... 224
user identity ... 205
provision Kerberos external authentication server ... 226
variable definitions ... 226

provision LDAP external authentication server 224
variable definitions 224
provision RADIUS external authentication server 225
variable definitions 225

R

Real-Time Reporting 149, 151
configure 149
procedure job aid 151
variable definitions 151
Real-Time Reporting (email contacts) 296
outbound contacts 296
Real-Time Reporting (outbound contacts) 301
outbound contacts 301
real-time traffic reports by contact 311
view 311
recipient mailbox 329, 333
change 329
create 329
delete 333
record 133
voice segment 133
record information 103
PABX 103
recover 481, 531
failed archive or restore 481
scheduled backup 531
reenable 238
user account 238
Reference Client 274
refresh 115, 126, 247
Alarm Monitor 115
service status 126, 247
reinstate 556
high availability 556
related resources 28
Avaya Mentor videos 28
reload data 234
UCM backup 234
remove 69, 138, 139, 213, 308, 313, 314
administrators 308
all silence from a voice segment 138
all silence from all voice segments 139
elements from a role 213
specified length to all voice segments 138
Web communications comfort groups 314
WC skillset 314
Web On Hold comfort groups 313
WC skillset 313
Web service package 69
remove attachments 344
prepared responses 344
rename 131
voice file 131
rename the name or IP address 565
Avaya Media Server server 565
replication 183, 187
AD-LDS 183
start 187
stop 187
reporting credentials 306
configure 306
reports 295, 298
email traffic 295
traffic 298
reset 93, 236, 454, 520, 589, 612
agent password 454
desktop password 93
grace period 520
iceAdmin password 589, 612
user password 236
reset user password 237
variable definitions 237
resource bulk 279
management 279
resource bulk management 280, 281, 284–286
export bulk resources 286
import bulk resources 285
import CS1000 data 281
import Windows users 280
import workstations from the domain 284
resource management 279
prerequisites 279
restore 93, 132, 141, 480, 531
archive 480
backup 531
user access to the server 93
voice file 132
voice segment marked for deletion 141
restore a backup 532, 533
procedure job aid 533
variable definitions 532
revert 130
voice file (existing) 130
review 548
shadowing 548
role 209, 215, 216
assign user 216
create 209
manage 209
mapping 215
root certificate authority to a file 200

save 200
root certificate authority to Internet Explorer 200
import 200
route data 182
capture 182
route point 378, 390
fax skillset 390
configure 390
scanned document skillset 378
configure 378
route point for a voice mail skillset 366
configure 366
route point for an SMS skillset 414
configure 414
routing table assignments 262
configure 262
routing tables 261
configure 261
RTD Multicast settings 450
configure 450
rule groups 293, 352
change 352
create 352
email 293
rules 347, 350, 351
change 347
create 347
delete 351
disable 351
enable 350

S

save 200
root certificate authority to a file 200
save a list of events 109
Event Browser 109
scanned document 377
configure 377
scanned document configuration 377–383, 385, 386
add document imaging server 379
add scanned document mailbox 381
configure route point 378
scanned document skillset 378
configure scanned document reply mailbox 383
delete document imaging server 380
delete scanned document mailbox 383
delete scanned document reply mailbox 385
prerequisites 377
update document imaging server 379
update scanned document 385, 386
system default rule 385
system delivery failure rule 386
update scanned document mailbox 382
scanned document mailbox 381–383
add 381
delete 383
update 382
scanned document reply mailbox 383, 385
configure 383
delete 385
scanned documents system default rule 385
update 385
scanned documents system delivery failure rule 386
update 386
schedule 529
backup of the database 529
schedule backup of the database 530
variable definitions 530
scheduled backup 531
recover 531
Screen Pops 465
configure 465
search 407
users in Active Directory 407
secured element 230, 231
delete 231
edit 230
security 495
fundamentals 495
Security Configuration Wizard 499
Windows Server 2008 Release 2 499
Security Framework 197, 199, 205
configure 197
disable 199
user identity provisioning 205
Security Framework configuration 197–202
configure CCMA security details 198
configure security prompts in Internet Explorer 201
disable Security Framework 199
import root certificate authority to Internet Explorer 200
prerequisites 197
save root certificate authority to a file 200
view security server settings 202
security fundamentals 495–498
CCMS Utility 498
view CCMS events 498
Event Browser and Alarm Monitor 496
Event severity 496
Event viewer settings 495
logon warning message CCMA 497
logon warning message UCM 497

SNMP 495
Systems Management Server security file (Multimedia) 497
security log 233
download and inspect 233
inspect 233
manage 233
security log management 234
reload data 234
UCM backup 234
security policy for passwords 217
create 217
security prompts in Internet Explorer 201
configure 201
security server settings 202
view 202
Security Templates 503, 504, 506
activate the Contact Center security template 503
apply the security template 504, 506
locally on the server 504
network domain 506
Windows Server 2008 Release 2 503
select 356, 516, 517
CCMA, CCT and CCMM events to be forwarded 517
CCMS events to be forwarded 516
outgoing email address 356
sender group 345–347
change 345
create 345
delete 346
delete sender 347
serial connection 174
extract data 174
Serial port 97
configure 97
view 97
server name 563
change 563
server name change 587, 593, 607, 611, 627, 640
CCMA 607
verify 587, 593, 611, 627, 640
server names or IP addresses change 564
prerequisites 564
server resources 101
view 101
Server utility 84, 85, 91–95
add desktop user accounts 91
change properties of desktop users 94
delete desktop user accounts 95
log off users 85
prevent users from accessing the server 92
print list of connected users 84
print list of users 95
reset desktop password 93
restore user access to the server 93
set privileges for users 85
view list of connected users 84
Server Utility 107, 112, 115–117, 119
Alarm Monitor behavior 116, 117
appears in background 117
appears in foreground 116
open Alarm Monitor 115
start 119
Provider 119
start Event Browser 107
throttle all events 112
Service Monitor 123, 124, 245, 246
close 246
configure 123, 245
start 124
Service Monitor configuration 124–126, 245–247
add site 247
change site to monitor 246
change the site to monitor 125
close Service Monitor 246
configure default site information 126
exit Networking Service Monitor 125
prerequisites 124, 245
refresh service status 126, 247
set default site information (client machine) 247
starting Service Monitor 124
service monitoring 544
configure 544
Service Packs 511
verify 511
service status 126, 247
refresh 126, 247
services 561
disable 561
enable 561
session 241
management 241
session management 241
ending sessions manually 241
view active sessions 241
set 247
default site information (client machine) 247
set privileges 85
users 85
set privileges for users 86
procedure job aid 86
settings 294, 495

Event viewer 495
inbound email 294
outbound email 294
setup 184
AD-LDS replication 184
setup AD-LDS replication 186
procedure job aid 186
shadowing 548
review 548
shadowing on a Mission Critical Standby Server 553
start 553
shared folder to export historical reports 156
create 156
shorten 137
voice segment 137
silence from a voice segment 138
remove 138
site 247
add 247
site in CCMA 253
add 253
site information 257
synchronize 257
site to monitor 125, 246
change 125, 246
site to the NCC 250
add 250
skillset 478
archive 478
skillsets for email 328
configure 328
SMS 413
configure 413
SMS configuration 413–416, 418, 419, 421, 422
add SMS Gateway 415
add SMS mailbox 416
configure a route point 414
SMS skillset 414
configure SMS reply mailbox 419
delete SMS Gateway 416
delete SMS mailbox 419
delete SMS reply mailbox 421
prerequisites 413
update SMS Gateway 415
update SMS mailbox 418
update SMS system default rule 421
update SMS system delivery failure rule 422
SMS Gateway 415, 416
add 415
delete 416
update 415
SMS mailbox 416, 418, 419
add 416
delete 419
update 418
SMS reply mailbox 419, 421
configure 419
delete 421
SMS system default rule 421
update 421
SMS system delivery failure rule 422
update 422
SMTP server on CCMA server 154
configure 154
SNMP 515
administration 515
SNMP administration 515–518
configure NMS 518
install Windows SNMP Service 515
select CCMA, CCT and CCMM events to be forwarded 517
select CCMS events to be forwarded 516
sort events 108, 116
Alarm Monitor 116
Event Browser 108
specify 459
email attachment size 459
SQL statement 36, 37, 71
SELECT...INTO 37
SET NOCOUNT ON 36
update 71
SQL statements or stored procedures 70, 72
construct and test 70
delete 72
SSL 359, 361
Email Manager 359
SMTP authentication 361
standby auto startup mode 555
Mission Critical HA 555
start 106, 119, 121, 124, 187, 476, 553, 559, 560
archive utility 476
Contact Center applications 559
Event Browser 106
individual services 560
Mission Critical Active Server 553
PC Event Browser 121
Provider 119
replication 187
Service Monitor 124
shadowing on a Mission Critical Standby Server 553
start Event Browser 106
procedure job aid 106

stop 187, 554, 559, 560
Contact Center applications 559
High Availability on a Mission Critical active server 554
High Availability on a Mission Critical standby server 554
individual services 560
replication 187
stored procedures 36
create 36
database integration service functionality 36
suggested responses 344
promote 344
support 19, 22–25, 28
agent-supervisor observe and barge-in 23
blind transfer 23
contact 28
geographic alternate CCT server 24
High Availability 19
inline attachments 22
Phonebook LDAP server 24
Screen Pops 24
Web communications comfort groups 22
Web On Hold comfort groups 22
WebLM licensing 22
Windows Server 2008 Release 2 25
switchover information 547
monitor 547
synchronize 257
site information 257
synchronize the operating system name 569, 587
CCMS name 569, 587
system data source names 63
configure 63
system default rule 334
update 334
system delivery failure rule 336
update 336
system license 306
configure 306

T

text chat labels 428
configure 428
throttle 112
events 112
TN data 178
capture 178
traffic 298
reports 298

U

UCM 497
logon warning message 497
UCM backup 234
reload data 234
update 71, 334, 336, 367, 370, 372, 373, 379, 382, 385, 386, 391, 394, 397, 398, 415, 418, 421, 422, 521, 570, 578, 579, 588, 594, 602–605, 613–615, 620–622, 627, 634, 641, 642, 649
client browsers and shared folders 594, 605, 614, 621
document imaging server 379
email attachment folders 642
fax 397, 398
system default rule 397
system delivery failure rule 398
fax mailbox 394
fax server 391
HOSTS file 570, 579, 588, 603, 615, 622, 627, 634, 641, 649
HOSTS file for clients 594, 604, 613, 620
license file 521
NCC server 578, 602
scanned document 385, 386
system default rule 385
system delivery failure rule 386
scanned document mailbox 382
SMS Gateway 415
SMS mailbox 418
SMS system default rule 421
SMS system delivery failure rule 422
SQL statement 71
system default rule 334
system delivery failure rule 336
voice mail mailbox 370
voice mail server 367
voice mail system default rule 372
voice mail system delivery failure rule 373
update CCMM server information in CCMA 646
variable definitions 646
update client browsers and shared folders 595, 606, 615, 622
variable definitions 595, 606, 615, 622
update the CCMM server IP address in CCMA 650
variable definitions 650
update the system default rule 335
variable definitions 335
update the system delivery failure rule 337
variable definitions 337
update voice mail system default rule 373
variable definitions 373

update voice mail system delivery failure rule 374
variable definitions 374
use 36, 37
SQL statement 36
stored procedure 37
SELECT...INTO 37
stored procedures 37
Oracle 37
user 215, 471
assign role 215
configure 471
user access to the server 93
restore 93
user account 237, 238
delete 238
disable 237
reenable 238
user accounts 235
manage 235
user configuration 471
User Settings page 471
user identity 205
provision 205
user identity provisioning 205, 206
add external account (optional) 206
add local user identity and password 205
user password 236
reset 236
user passwords 235
manage 235
User Settings 471
page 471
users 85
log off 85
set privileges 85
users from accessing the server 92
prevent 92
users in Active Directory 407
search 407
utility 31
CCMS configuration 31
Nbconfig 31

V

variable definitions 43, 45, 47, 49, 51, 58, 81, 112, 151, 154, 156, 159, 164, 198, 206, 207, 210, 212, 224–226, 230, 236, 237, 276, 278, 281, 285, 322, 326, 330, 332, 335, 337, 338, 342, 346, 349, 353, 366, 369, 373, 374, 378, 381, 384, 390, 393, 396, 410, 414, 417, 420, 427, 429, 430, 450, 460, 467, 526, 528, 530, 532, 534, 535, 540, 542, 543, 546, 548, 550, 552, 570, 578, 588, 595, 602, 606, 612, 615, 620, 622, 627, 634, 640, 645, 646, 649, 650
add a new Contact Center application 230
add event preference 112
add external account (optional) 207
add fax mailbox 393
add local user identity and password 206
add scanned document mailbox 381
add SMS mailbox 417
add voice mail mailbox 369
Agent Desktop Displays parameters on the server 159
assign a development Web server name 427
CCT licensing configure 276
change admin password 236
change CS 1000 PABX data 47
change IP multicast setting 58
change licensed features configuration 45
change local settings configuration 43
change SIP Local Subscriber data 49
change SIP Network Settings data 51
co-resident server name change 588
configure a route point 414
SMS skillset 414
configure a route point for an SMS skillset 414
configure Agent Desktop 645
configure Agent Desktop Advanced Settings 467
configure Agent Desktop behavior 460
configure CCMA security details 198
configure CCT deployment type 278
configure contact timers 430
configure email server names 326
configure fax reply mailbox 396
configure Integrated Reporting 535
configure Mission Critical High Availability on the active server 550
configure Mission Critical High Availability on the standby server 552
configure notification of automatic switchovers 543
configure predictive blending settings 450
configure route point 378, 390
fax skillset 390
scanned document skillset 378
configure route point for a voice mail skillset 366
configure route point for an Outbound skillset 322
configure scanned document reply mailbox 384
configure service monitoring 546
configure SMS reply mailbox 420
configure SMTP server on CCMA server 156
configure warm standby or hot-standby managed IP address 540

configure warm standby or hot-standby server .. 542
configure welcome messages and text chat labels 429
create backup location 526
create custom role 210
create expert group 410
create or change a keyword group 338
create or change an alias for a recipient mailbox 332
create or change prepared responses 342
create or change recipient mailbox 330
create or change rule groups 353
create or change rules 349
create or change sender group 346
email notifications (Historical reporting) 154
import Windows users 281
import workstations from the domain 285
mapping elements and permissions to a role 212
migrate the database 534
monitor switchover information 548
network printer on the CCMA server 164
perform immediate backup of the database 528
preview list of access classes 81
provision Kerberos external authentication server 226
provision LDAP external authentication server .. 224
provision RADIUS external authentication server 225
Real-Time Reporting 151
reset user password 237
restore a backup 532
schedule backup of the database 530
update CCMM server information in CCMA 646
update client browsers and shared folders 595, 606, 615, 622
update the CCMM server IP address in CCMA . 650
update the system default rule 335
update the system delivery failure rule 337
update voice mail system default rule 373
update voice mail system delivery failure rule 374
verify the CCMA server IP address change 620
verify the CCMA server name change 612
verify the CCMM server IP address change 649
verify the CCMM server name change 640
verify the CCMS IP address change 578
verify the CCMS server name change 570
verify the CCT server IP address change 634
verify the CCT server name change 627
verify the server IP address change 602
verify 511, 587, 593, 611, 627, 640
server name change 587, 593, 611, 627, 640
Service Packs 511
verify the CCMA server IP address change 620
variable definitions 620
verify the CCMM server IP address change 649
variable definitions 649
verify the CCMS IP address change 578
variable definitions 578
verify the CCT server IP address change 634
variable definitions 634
verify the server IP address change 602
variable definitions 602
videos 28
Avaya Mentor 28
view 84, 97, 101, 108, 202, 241, 311
active sessions 241
list of connected users 84
online Help for an event 108
real-time traffic reports by contact 311
security server settings 202
Serial port 97
server resources 101
view CCMS events 498
CCMS Utility 498
view members 79
access classes 79
voice contacts 24
configure Phonebook LDAP server 24
Voice Contacts 24
enable Customer History 24
voice file 129–132
copy 131
create 129
delete 131
open 130
rename 131
restore 132
voice file (existing) 130
revert 130
voice mail 365
configure 365
voice mail configuration 365–368, 370–373
add voice mail mailbox 368
add voice mail server 367
configure route point for a voice mail skillset 366
delete voice mail mailbox 371
delete voice mail server 368
prerequisites 365
update voice mail mailbox 370
update voice mail server 367
update voice mail system default rule 372
update voice mail system delivery failure rule 373
voice mail mailbox 368, 370, 371
add 368

delete ... 371
update ... 370
voice mail server ... 367, 368
add ... 367
delete ... 368
update ... 367
voice mail system default rule ... 372
update ... 372
voice mail system delivery failure rule ... 373
update ... 373
voice port data ... 179
capture ... 179
Voice Prompt Editor ... 127–129
configure ... 127
log off ... 129
log on ... 128
Voice Prompt Editor configuration ... 127–141
copy voice file ... 131
create voice file ... 129
create voice segment ... 132
delete voice file ... 131
delete voice segment ... 140
lengthen or shorten a voice segment ... 137
log off the Voice Prompt Editor ... 129
log on to Voice Prompt Editor ... 128
open voice file ... 130
play a group of voice segments ... 135
play voice segment ... 134
prerequisite ... 127
record voice segment ... 133
remove all silence from a voice segment ... 138
remove all silence from all voice segments ... 139
remove or add a specified length to all voice segments ... 138
rename voice file ... 131
restore voice file ... 132
restore voice segment marked for deletion ... 141
revert to an existing voice file ... 130
search voice segment ... 136
voice segment ... 132–134, 136, 137, 140
create ... 132
delete ... 140
lengthen ... 137
play ... 134
record ... 133
search ... 136
shorten ... 137
voice segment marked for deletion ... 141
restore ... 141

W

warm standby or hot-standby automatic switchovers 547
configure ... 547
warm standby or hot-standby managed IP address ... 539
configure ... 539
warm standby or hot-standby manual switchovers ... 544
configure ... 544
warm standby or hot-standby server ... 541
configure ... 541
Web communications ... 425
configure ... 425
Web Communications ... 432
transfer to skillset ... 432
Web communications comfort group ... 444
delete ... 444
delete message ... 444
Web communications comfort groups ... 442
create ... 442
Web On Hold comfort group ... 440
delete message ... 440
Web On Hold comfort groups ... 439
create ... 439
Web On Hold URL group ... 437, 438
delete ... 438
delete URL ... 437
Web On Hold URLs groups ... 436
create ... 436
Web service package ... 69
remove ... 69
Web services ... 68
configure ... 68
welcome messages ... 402, 428
configure ... 402, 428
Windows SNMP Service ... 515
install ... 515
Windows time service ... 510
disable ... 510
Windows users ... 280
import ... 280
workstations from the domain ... 284
import ... 284

X

XML Automated Assignments feature ... 167
install ... 167