Avaya Aura™ Contact Center

Server Administration

NN44400-610

Document status: Standard
Document issue: 02.07
Document date: 02 March 2011
Product release: Release 6.0/6.1
Job function: Administration
Type: Technical Publication
Language type: English

Copyright © 2011 Avaya Inc.
All Rights Reserved.

Notices
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
Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree 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(s) 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 this product. 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://www.avaya.com/support
Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said 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, AND 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 the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) 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. 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(s) 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(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party. Avaya is a registered trademark of Avaya Inc. All non-Avaya trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support. Web site: http://www.avaya.com/support

Contact Avaya Support
Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

New in this release 17
Features 17
Multimedia Administrator application 17
New multimedia contact types 18
Real-time traffic reports for media types 18
Automatic suggestions for agents 19
Recording out of office hours 19
High Availability 19
SIP-enabled contact center features 20
Communication Control Toolkit client and server administration 20
Communication Control Toolkit automatic resource assignment 21
Multiplicity 22
Active Directory Lightweight Directory Services 22
Other changes 23
Windows Server 2008 Release 2 support 23
Introduction 25
Prerequisites 25
Contact Center Manager Server fundamentals 27
Configuration utility 27
Database Integration service functionality 28
Interaction of the Database Integration service with HDX 28
Interaction with application commands 29
Stored procedures 32
Feature report 33
Multicast Address and Port Configuration 34
Multicast Stream Control 34
Server configuration 34
Web services 34

Contact Center Manager Server 37
Contact Center Manager Server configuration 39
Starting the Configuration utility with regular access level 39
Starting the Configuration utility with administration access level 40
Changing the local settings configuration 40
Changing the licensed features configuration 42
Changing the Avaya Communication Server 1000 PABX data 44
Contact Center Manager Server statistics configuration 47
Configuring the Multicast controller 47
Changing the IP multicast settings 48
Disconnecting Terminal Services sessions 50

Database Integration Wizard configuration 51
Creating and invoking a stored procedure 52
Configuring the system data source names 53
Configuring HDX and TAPI server settings 55
Configuring the database connections 58
Configuring Web services 59
Removing a Web service package 60
Constructing and testing SQL statements or stored procedures 61
Updating an SQL statement 62
Deleting an existing SQL statement or stored procedure 62
Configuring the Contact Center Manager Server script 63
Backing up the Database Integration Service 64
Restoring the configuration 65

Contact Center Manager Server Utility 67
Access Class operations 69
Logging on to Server Utility 70
Creating an access class 70
Viewing members of an access class 71
Modifying access class properties 72
Previewing the list of access classes 73
Printing the list of access classes 73
Deleting an access class 74
Connected user and user account operations 75
Viewing a list of connected users 76
Printing a list of connected users 76
Logging off a user 77
Setting privileges for a user 77
Adding desktop user accounts 84
Preventing users from accessing the server 85
Restoring access to the server for a user 85
Resetting desktop passwords 86
Changing the properties of a desktop user 88
Printing a list of users 88
Deleting a desktop user 89
Serial port configuration 91
Viewing port settings 92
Printing port settings 92
Editing port settings 93
Server settings 95
Viewing server resources 95
Printing server resources information 96

PABX configuration 97
Recording PABX information 97
Alarm and Event configuration 99
Starting the Event Browser 100
Starting the Event Browser from Server Utility 101
Sorting events in the Event Browser 102
Viewing online Help for an event 102
Saving a list of events 102
Printing a list of events 103
Changing the filtering criteria for events 104
Adding an event preference 105
Throttling all events 106
Changing an event preference 107
Printing the list of event preferences 107
Deleting an event preference 107
Changing the classification of an event 108
Opening the Alarm Monitor 108
Refreshing the Alarm Monitor 109
Sorting events in the Alarm Monitor 109
Specifying when the Alarm Monitor appears in the foreground 110
Configuring the Alarm Monitor to appear in the background 110
Obtaining more information about an alarm 111
Manually clearing an alarm 111
Provider configuration 113
Starting the Provider 113
Connecting to the Contact Center Manager Server 113
PC Event Browser configuration 115
Starting the PC Event Browser 115
Contact Center Service Monitor configuration 117
Starting Contact Center Service Monitor 118
Changing the site to monitor 119
Exiting Networking Service Monitor 119
Refreshing the service status 119
Configuring the default site information 120
Voice Prompt Editor configuration 121
Logging on to the Voice Prompt Editor 122
Logging off the Voice Prompt Editor 122
Creating a voice file 123
Opening a voice file 123
Reverting to a previously saved voice file 124
Copying a voice file 124
Renaming a voice file 124
Deleting a voice file 125
Restoring a voice file 125

Creating a voice segment 126
Recording a voice segment 126
Playing a voice segment 127
Playing a group of voice segments 128
Searching for a voice segment 128
Lengthening or shortening a voice segment 129
Removing all silence from a voice segment 130
Removing or adding a specified length to all voice segments 131
Removing all silence from all voice segments 132
Deleting a voice segment 133
Restoring a voice segment marked for deletion 133

Contact Center Manager Administration 135

Contact Center Manager Administration configuration 137

Configuring the Contact Center License Manager Service 138
Configuring your logon warning message title and text 139
Enabling the logon warning message 140
Configuring Real-Time Reporting 141
Configuring Emergency Help 143
Configuring e-mail notifications for Historical reporting 144
Configuring SMTP Server on the Contact Center Manager Administration 146
Server 146
Creating a shared folder to export historical reports 147
Installing the Service Creation Environment 149
Configuring Agent Desktop Display parameters on the server 150
Changing the password for the iceAdmin user account 153
Configuring the LPR port for printers 154
Configuring a network printer on the CCMA server 154
Configuring a network printer to use the CCMA server as the print server 156
Configuring a network printer to use a print server other than the CCMA server 157
Installing the XML Automated Assignments feature 158
Configuring Avaya Call Recording and Quality Monitoring 159
Configuring CDN Landing Pads for Universal Networking or Integrated Reporting 160
Configuring a DNIS Landing Pad for Universal Networking 161

Avaya Communication Server 1000 Data Extraction Tool operation163

Extracting data from a serial connection 164
Extracting data using a modem 165
Extracting data from a file 166
Capturing Terminal Number data 167
Capturing voice port data 169
Capturing CDN data 169
Capturing IVR ACD-DN data 170
Capturing route data 171

CCMA and Security Framework backup and restore 173
Backing up Contact Center Manager Administration 175
Backing up Security Framework 179
Viewing scheduled tasks in the Backup and Restore utility 181
Recording Real-Time Reporting and Emergency Help configurations 182
Restoring Contact Center Manager Administration data 182
Restoring Security Framework data 185
Switching to the standby server in Agent Desktop Display 186
Active Directory Lightweight Directory Services replication 187
Setting up AD-LDS replication 188
Choosing AD-LDS service accounts 190
Stopping replication on replicating servers 191
Starting replication on replicating servers 191
Contact Center Manager Administration failure recovery 193
Restoring the Contact Center Manager Administration database 195
Language support fundamentals 197
Language levels 197
International environment 197
International and local environment 198
Language family compatibility 198
Security Framework configuration 201
Obtaining a server certificate from the Security Framework 202
Obtaining a server certificate from a third-party authority 203
Installing a server certificate 204
Configuring the Contact Center Manager Administration security details 204
Disabling the Security Framework 206
Saving the root certificate authority to a file 206
Importing the root certificate authority to Internet Explorer 207
Configuring security prompts in Internet Explorer 207
Viewing the security server settings 208

Security Commissioning 209
User identity provisioning 211
Adding a local user identity and password 211
Adding an external account (optional) 212
Role creation and management 215
Creating a custom role 215
Deleting a custom role (optional) 216
Element and permission mapping 217
Mapping elements and permissions to a role 217
Mapping elements and permissions by copying from another role 218
Removing elements from a role (optional) 219

Role mapping 221
Assigning roles to a user 221
Assigning users to a role 222
Policy creation and management 223
Creating a security policy for passwords 223
External identity repository configuration 227
Provisioning an LDAP authentication server 228
Provisioning a RADIUS authentication server 229
Provisioning a Kerberos authentication server 230
Creating an authentication scheme 231
Element Management 233
Adding a new Contact Center application (Optional) 233
Editing a secured element (optional) 234
Deleting a secured element (Optional) 234
Security log management 237
Inspecting security logs 237
Downloading and inspecting security logs 237
Account and password management 239
Changing your password 239
Resetting a user password 240
Disabling a user account (optional) 241
Reenabling a user account (optional) 241
Deleting a user account (optional) 242
Session management 243
Viewing active sessions 243
Ending sessions manually 243

Network Control Center Server 245
Networking Service Monitor configuration 247
Changing the site to monitor 247
Closing the Networking Service Monitor 248
Refreshing the service status 248
Setting the default site information (client machine) 249
Adding a site 249
Network Control Center server administration 251
Adding a site to the NCC 252
Adding access classes 253
Adding a site in Contact Center Manager Administration 254
Configuring network communication parameters 255
Synchronizing site information 257
Adding a network skillset 258
Configuring network skillset properties 259
Configuring Agent Order Preference 260

Configuring the routing tables 260
Configuring routing table assignments 261
Configuring the historical statistics collection 263
Configuring MCDN network CDNs 263
Configuring DNIS Network CDNs 265

Communication Control Toolkit Server 267
Communication Control Toolkit fundamentals 269
Automatic Call Distribution 269
Communication Control Toolkit Administration tool (CCT Console and Web Administration) 270
Contact Management Framework 270
Trace Control Utility 270
Resources 270
Resource Assignments 271
Programming interfaces 272
Application programming interface 272
Web services 273
Communication Control Toolkit Reference Client 274
Server settings configuration 275
Configuring the licensing for CCT 275
Configuring the deployment type for CCT 276
Configuring the Avaya Communication Server 1000 service provider 278
Resource management 281
Importing Windows users from the Communication Control Toolkit domain 281
Importing Avaya Communication Server 1000 data 283
Importing workstations from the domain 286
Adding resources manually 287
Changing the properties of a resource 289
Assigning resources 289
De-assigning resources 291
Deleting resources 292
Importing bulk resources 292
Exporting Bulk Resources 293
Configuring Hotdesking (Agent Roaming) 295

Contact Center Multimedia 297
Contact Center Multimedia fundamentals 299
E-mail contact type 300
E-mail rule groups 301
Recipient mailboxes 302
Inbound e-mail settings 302
Outbound e-mail settings 302
Character encoding for outgoing e-mail messages 302

Asian e-mail 303
E-mail traffic reports 303
Agent Desktop 304
Contact Center Manager Administration 304
Web services 304
SMS text messages, faxes, scanned documents and voice mail attachments 305
Mailbox configuration 306
Traffic reports 306
Agent Desktop 306
Outbound contact type 307
Outbound Campaign Management Tool 308
Campaign Scheduler 308
Agent Desktop 308
Contact Center Manager Administration 309
Web services 309
Web communications 309
Instant Messaging 310
Office hours 310
General configuration 311
Configuring the system license 311
Configuring the reporting credentials 312
Adding administrators 312
Removing administrators 313
Configuring office hours 314
Configuring holidays 315
Applying office hours 315
Viewing real-time traffic reports by contact 316
Configuring the displayed date for traffic reports 317
Outbound configuration 319
Configuring a route point for an Outbound skillset 319
E-mail configuration 321
Configuring the e-mail server names 323
Adding an e-mail server 324
Deleting an e-mail server 325
Configuring skillsets for e-mail 325
Creating or changing a recipient mailbox 326
Creating or changing an alias for a recipient mailbox 329
Deleting a recipient mailbox 331
Updating the system default rule 331
Updating the system delivery failure rule 333
Creating or changing a keyword group 335
Deleting a keyword from a keyword group 337
Deleting a keyword group 338
Creating or changing prepared responses 338

Deleting prepared responses 341
Removing attachments from prepared responses 342
Promoting suggested responses 342
Creating or changing a sender group 343
Deleting a sender group 344
Deleting a sender from a sender group 345
Creating or changing rules 345
Enabling a rule 348
Disabling a rule 349
Deleting a rule 349
Creating or changing rule groups 350
Configuring the e-mail settings 351
Changing the character encoding for outgoing e-mail 354
Changing the character encoding of e-mail replies 355
Selecting the outgoing e-mail address 356
Barring e-mail addresses 356
Deleting a barred e-mail address 357
Configuring Microsoft Exchange 2007 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 361
Voice Mail configuration 365
Configuring a route point for a voice mail skillset 365
Adding a voice mail mailbox 366
Fax configuration 369
Configuring a route point for a fax skillset 369
Adding a fax mailbox 370
Configuring reply addresses 372
Scanned document configuration 375
Configuring a route point for a scanned document skillset 375
Adding a scanned document mailbox 376
Configuring reply addresses 378
SMS configuration 381
Configuring a route point for a SMS skillset 382
Adding an SMS mailbox 382
Configuring reply addresses 384
Web communications configuration 387
Assigning development Web server name 388
Configuring welcome messages and text chat labels 389
Configuring customer notification log 390
Configuring contact timers 391
Creating automatic phrases 392
Deleting an automatic phrase 393
Creating a page push URL 394

Deleting a page push URL 394
Creating Web On Hold URLs groups 395
Changing the sequence of a Web On Hold group 396
Deleting a URL from a Web On Hold group 396
Deleting a Web On Hold group 397
Web communications customer interface configuration 399
Using the sample customer interface Web site 400
Configuring properties for the sample customer interface Web site 409
Testing the customer interface Web site 411
Creating a test customer 411
Testing request text chat 412
Testing the request callback 413
Testing e-mail from Web pages 414
Instant message configuration 415
Configuring welcome and disconnect messages 415
Creating automatic phrases 416
Deleting an automatic phrase 417
Creating a page push URL 418
Deleting a page push URL 419
Predictive Outbound administration 421
Configuring predictive blending settings 421
Configuring RTD Multicast settings 424
Configuring predictive outbound agent scripts 425
Agent Desktop configuration 427
Resetting an agent password 428
Configuring agent access to contacts 428
Controlling access to e-mail message text 429
Creating or changing custom fields in Agent Desktop 429
Deleting a custom field in Agent Desktop 430
Configuring the active contact timer 430
Configuring the callback timer 431
Configuring the callback trunk access 432
Specifying the attachment size 432
Configuring Agent Desktop behavior 433
Configuring the state of the Agent terminal on log off 434
Configuring hotdesking 435
Configuring hotdesking in a Citrix environment 435
Creating or changing a closed reason 436
Configuring default closed reasons 436
Deleting a closed reason 437
Importing an Active Directory user to CCMM 437
Creating an expert group 438
Adding an agent to an expert group 439
Deleting an agent from an expert group 440

Deleting an agent from a skillset associated group 440
Configuring an Auto Launch application 441
Configuring Intrinsic settings 441
Data collection and management 443
Starting the archive utility 444
Archiving by outbound campaign 444
Archiving by e-mail rule 445
Archiving by skillset 446
Archiving by closed reason 447
Restoring an archive 448
Recovering from a failed archive or restore 448
Security Fundamentals 451
Simple Network Management Protocol 452
Event viewer settings 452
Event Severity 452
Security template 453
Event Browser and Alarm Monitor 453
Logon warning message (CCMA and UCM) 453
Systems Management Server security file (Multimedia) 454
Group policy 454
Contact Center Manager Server Utility to view events on CCMS 454
Platform Security 455
Securing the Server 455

Managing Security 459
Security Template 461
Activating the Contact Center security template 462
Applying the security template locally on the server 463
Applying the security template in a network domain 464

Common server administration 467
Microsoft Windows configuration and management 469
Managing date and time features 469
Disabling the Windows time service 470
Verifying Service Packs 470
Adding a server to a domain 471
Configuring the operating system for remote access in a domain 472
Configuring the operating system for remote access in a workgroup 473
Simple Network Management Protocol administration 475
Installing Windows SNMP Service 475
Selecting CCMS events to be forwarded 476
Selecting CCMA, CCT, and CCMM events to be forwarded 477
Configuring the NMS 477

Licensing administration 479
Resetting the grace period 479
Updating the license file 480
Changing from Nodal to Corporate licensing 481
Changing the license manager file on a Contact Center Manager Server 482
Refreshing your server 483
Contact Center database maintenance 485
Creating a backup location 486
Performing an immediate backup of the database 487
Scheduling a backup of the database 489
Recovering a scheduled backup 490
Restoring a backup 491
Migrating the database 493
Configuring Integrated Reporting 494
Contact Center server High Availability 497
Configuring managed IP addresses 498
Configuring the standby server 500
Configuring the notification of automatic switchovers 501
Configuring manual switchovers 502
Configuring service monitoring 503
Configuring automatic switchovers 506
Monitoring switchover information 506
Reviewing shadowing 507
Common procedures 509
Starting or stopping Contact Center applications 509
Stopping individual services 510
Starting individual services 510
Disabling services 510
Enabling services 511
Adding a server to a domain 512

Appendix 513
Server name or IP address change 515
CCMS server name change 515
Changing the server name on the operating system 517
Verifying the server name change 517
Synchronizing the operating system name with the CCMS name 518
Updating the HOSTS file 519
Changing the server name in the Administration tool 519
Configuring the Contact Management Framework settings 520
Configuring the Multimedia server settings 521
CCMS server IP address change 522
Changing the contact center subnet IP address 523

Configuring the Contact Center Manager Server 524
Verifying the IP address change 524
Updating the Network Control Center server 525
Updating the HOSTS file 526
Updating the server IP address in CCMA 526
Changing the Contact Center License Manager IP address 527
Updating the Communication Control Toolkit license 528
Changing the ELAN subnet IP address 528
Co-resident server name change 530
Changing the server name in the operating system 532
Verifying the server name change 533
Updating the HOSTS file 533
Synchronizing the operating system name with the CCMS name 534
Resetting the IUSR_SWC account 534
Resetting the iceAdmin password 536
Updating client browsers and shared folders 536
Configuring destination for exported scheduled reports 537
Changing the server name in the Administration tool 538
Updating the HOSTS file for clients 539
Configuring the Contact Management Framework 539
Configuring the Multimedia server settings 540
Co-resident server IP address change 542
Changing the contact center subnet IP address of the co-resident server 543
Configuring the co-resident server IP address 544
Verifying the server IP address change 544
Updating the Network Control Center server 545
Updating the HOSTS file 545
Updating the server IP address in CCMA 546
Updating the HOST file for clients 547
Updating client browsers and shared folders 548
Changing the Contact Center License Manager IP address 549
Updating the Communication Control Toolkit server IP address in CCMA 549
Updating the Communication Control Toolkit Provider IP address 550
CCMA server name change 551
Changing the server name in the operating system 553
Verifying the server name change 553
Resetting the iceAdmin password 554
Updating historical report output files 555
Updating the HOSTS file for clients 555
Updating client browsers and shared folders 556
Updating the HOSTS file 557
Configuring the Multimedia server settings 558
CCMA server IP address change 559
Changing the server IP address on the server 560

Verifying the server IP address change 560
Updating the HOSTS file for clients 561
Updating client browsers and shared folders 562
Updating the HOSTS file 563
CCT server name change 564
Changing the server name on the operating system 566
Verifying the server name change 566
Synchronizing the operating system name with the CCT name 567
Updating the HOSTS file 568
Configuring the deployment type for CCT 568
Configuring Contact Center Manager Server 570
Configuring the Multimedia server settings 571
Configuring the Agent Desktop 571
CCT server IP address change 573
Changing the server IP address on the operating system 574
Verifying the server IP address change 574
Updating the HOSTS file 575
CCMM server name change 576
Changing the server name on the operating system 578
Verifying the server name change 578
Updating the HOSTS file 579
Configuring the Multimedia server settings 580
Updating the e-mail attachment folders 581
Configuring the external Web server 582
Configuring the Agent Desktop 583
Updating the server information in Contact Center Manager Administration 583
CCMM server IP address change 585
Changing the IP address on the operating system 586
Verifying the server IP address change 586
Updating the HOSTS file 587
Updating the server information in Contact Center Manager Administration 588
Default login values 591

New in this release

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

- Features (page 17)
- Other changes (page 23)

Features

See the following sections for information about feature changes:

- Multimedia Administrator application (page 17)
- New multimedia contact types (page 18)
- Real-time traffic reports for media types (page 18)
- Automatic suggestions for agents (page 19)
- Recording out of office hours (page 19)
- High Availability (page 19)
- SIP-enabled contact center features (page 20)
- Communication Control Toolkit client and server administration (page 20)
- Communication Control Toolkit automatic resource assignment (page 21)
- Multiplicity (page 22)
- Active Directory Lightweight Directory Services (page 22)

Multimedia Administrator application

A new Contact Center Multimedia administrator application is started using the Contact Center Manager Administration application. You can perform all of the administration for your contact center from a single server instead of moving to the Multimedia server for configuration.

The new user interface gives the application a Web-like appearance and is organized by contact types.

The procedures for all multimedia resource configuration are changed to reflect the new software. For more information, see the following chapters:

- General configuration (page 311)
- Outbound configuration (page 319)
- E-mail configuration (page 321)
- Voice Mail configuration (page 365)
- Fax configuration (page 369)

- Scanned document configuration (page 375)
- SMS configuration (page 381)
- Web communications configuration (page 387)
- Instant message configuration (page 415)
- Predictive Outbound administration (page 421)
- Agent Desktop configuration (page 427)
- Data collection and management (page 443)

New multimedia contact types

You can use the Contact Center Multimedia server to interact with four new contact types. The existing Contact Center Multimedia e-mail routing manager routes the SMS, fax, scanned documents, and voice mail messages to agents based on the skillsets.

The new contact types require configuration for the skillsets in Contact Center Manager Administration, and route points for the default skillsets in the Multimedia Administrator.

Existing Instant messaging for the Session Initiated Protocol (SIP)-enabled environment have additional configurations.

For information about the new and changed contact types, see the following sections:

- Contact Center Multimedia fundamentals (page 299)
- Voice Mail configuration (page 365)
- Fax configuration (page 369)
- Scanned document configuration (page 375)
- SMS configuration (page 381)
- Instant message configuration (page 415)

Real-time traffic reports for media types

All contact types have current traffic reports configured to show the current status. The administrator can choose the time period to view traffic for each contact type and

- monitor the incoming and closure rate for a type of contact on defined or all skillsets for a selected date to determine if the traffic levels are being adequately managed.
- view the traffic levels for the date (new and closed contacts).
- view the average time a contact spent in queue while the contact center is open.

For more information about the traffic reports, see SMS text messages, faxes, scanned documents and voice mail attachments (page 305).

Automatic suggestions for agents

Contact centers are always aiming to add operational efficiency to the handling of contacts, whatever their type. With e-mail messages, the entire communication is received at the time of processing. A large volume of inbound e-mail messages generate similar responses and efficiency can be gained when the system suggests a response to the agent who accepts or declines the suggestion.

Administrators can review the auto suggestions and can promote them to an automatic response, where they are available throughout the contact center.

For more information, see

- Creating or changing prepared responses (page 338)
- Promoting suggested responses (page 342)

Recording out of office hours

To improve accuracy in the measurement of multimedia service levels, a mechanism is introduced to account for the regular hours of operation of the contact center and public holidays.

If a goal is to respond to an e-mail message within 6 hours, an e-mail arriving on Friday afternoon is reported as missed its service level if it is processed on the next working day (Monday). By accurately configuring out of office hours, the time that the contact center is closed can be removed from the interval between when the contact is queued and handled.

For more information, see

- Configuring office hours (page 314)
- Configuring holidays (page 315)

High Availability

High Availability (HA) supports hot standby 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 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. CCMA switchover will not happen automatically so you must manually change over to the standby CCMA if the primary CCMA fails.

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 (page 497).

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)
- Call Forward settings on agent telephones
- Music on hold for transfers

Let Call Ring as an option in the Call Presentation Class of Service is not supported for SIP-enabled contact center installations.

Communication Control Toolkit client and server administration

The CCT Snap-in has been updated to include server-side and bulk configuration tasks only. CCT Administration is done using the CCT Web Administration client, which is accessible from CCMA. This release contains several changes to Communication Control Toolkit (CCT):

- CCT Snap-in server configuration

  CCT Snap-in enables the user to configure the deployment type, License Configuration and CCT Web Services.

- CCT Snap-in bulk import and export tool

  The bulk provisioning tool has been updated to replace the Import Configuration and Export Configuration tools of the previous release. This tool provides the ability to export any or all data in the CCT database to an XML file using one of two possible XML schema definitions; a standard data schema definition and a flat schema definition.

  The flat schema definition file is suitable for use with Microsoft Excel. When a file is exported using this tool, the schema definition file (XSD file) for the selected export format is created in the output location, along with the requested export file.

  Due to changes made to the database schema in the current release, the file formats (both TAB and XML) used in the previous release are incompatible with the current Database Import/Export tool.

  The CCT Snap-in also provides Import Avaya Communication Server 1000 Data, Import Windows Users and Import Workstations.

- CCT contact center users are no longer managed by CCT.

  Contact center users are no longer managed using CCT administration tools. CCT contact center users, or agents, are managed using CCMA.

- CCT Web administration client

  Use the Communication Control Toolkit Web Administration client to configure the day-to-day administration for Contact Center. It allows the Administrator to perform add, delete, edit and assign functionality on the following resources:

  — Agent groups

  — Users, User Groups

  — Terminals, Terminal Groups

  — Addresses, Address Groups

  — Workstations

It also allows the Administrator to add, delete and edit IVRs and configure provider information.

Communication Control Toolkit automatic resource assignment

In this release CCT has updated the manually enabled auto-mapping feature to an automatic mapping feature. When a terminal is assigned to an agent, CCT automatically assigns the terminal's associated addresses to the respective agent. When the agent logs in, CCT checks any changes to the agent's configuration. Any new addresses assigned to the terminal are automatically assigned to the agent. Also, any un-assigned addresses, are automatically un-assigned from the respective agents. For specialized CCT behavior, an administrator can assign route point addresses to agents.

In the previous release, the auto-mapping feature was manually enabled in the CCT Snap-in, however the administrator had to remember to enable this feature. Now this feature is automatic.

Multiplicity

Multiplicity is a CCMS feature. Multiplicity is the term used by Avaya to describe the ability of an agent to handle multiple concurrent contacts. At any one time an agent can be active on a voice and multimedia contact simultaneously, however only one of these can be active, the others automatically go on hold.

The Multiplicity feature can be configured during installation or using the Multiplicity optional feature in Contact Center Server Configuration. Multiplicity is a licensed feature.

Active Directory Lightweight Directory Services

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).

Other changes

See the following sections for other changes in this release:

- Windows Server 2008 Release 2 support (page 23)

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 (page 137)
- Language support configuration (page 203)
- Common procedures (page 509)

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 6.0/6.1 servers after the initial configuration.

Prerequisites

- 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 6.0/6.1 software. See *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Commission your Contact Center Release 6.0/6.1 software. See *Avaya Aura™ Contact Center Commissioning* (NN44400-312).

Navigation

- Contact Center Manager Server (page 37)
- Contact Center Manager Server Utility (page 67)
- Contact Center Manager Administration (page 135)
- Security Commissioning (page 209)
- Network Control Center Server (page 245)
- Communication Control Toolkit Server (page 267)
- Contact Center Multimedia (page 297)
- Managing Security (page 459)
- Common server administration (page 467)

Contact Center Manager Server fundamentals

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

Navigation

- Configuration utility (page 27)
- Database Integration service functionality (page 28)
- Feature report (page 33)
- Multicast Address and Port Configuration (page 34)
- Multicast Stream Control (page 34)
- Server configuration (page 34)
- Web services (page 34)

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 regular access level (page 39)
- Starting the Configuration utility with administration access level (page 40)

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.

Attention: 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 TAPI call data attachment is 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, consult 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 (page 40)
- Changing the licensed features configuration (page 42)
- Changing the Avaya Communication Server 1000 PABX data (page 44)

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.

Contact Center Manager Server

- Contact Center Manager Server fundamentals (page 27)
- Contact Center Manager Server configuration (page 39)
- Certificate management for SIP-CCMS (page 49)
- Database Integration Wizard configuration (page 51)
- Contact Center Manager Server statistics configuration (page 47)

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:

- 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 (page 39)
- Starting the Configuration utility with administration access level (page 40)
- Changing the local settings configuration (page 40)
- Changing the licensed features configuration (page 42)
- Changing the Avaya Communication Server 1000 PABX data (page 44)

Starting the Configuration utility with regular access level

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 steps

Step	Action
1	Click **Start, Run**.
2	In the **Run** text box, type **nbconfig**.
3	Click each tab to view the content.

4 Click **OK**.

--End--

Starting the Configuration utility with administration access level

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

Procedure steps

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

--End--

Changing the local settings configuration

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 steps

Step	Action
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**.

--End--

Variable definitions

Variable	Value
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, 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

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 steps

Step	Action
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**.

--End--

Variable definitions

Variable	Value
CCMS Package	The installation package indicates the licenses that you purchased with Contact Center: • Nodal Enterprise: The base package for Contact Center on the current supported switching platforms. • Corporate Enterprise: The networking package. • Corporate NCC: The Network Control Center package for multiple Contact Center Manager Servers
CLAN Subnet IP Address	The IP address of the entire IP network including the ELAN subnet and the contact center subnet.
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.
Optional Packages	You must choose the package you purchased. Some packaged features includes: • 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 Universal Networking—Use Network Skill-Based Routing to route voice and multimedia contacts between networked sites in a mixed PABX environment.
Serial Number	The serial number for the Contact Center suite license manager. You must obtain the serial number from your distributor.

Changing the Avaya Communication Server 1000 PABX data

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 steps

Step	Action
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**.

--End--

Variable definitions

Variable	Value
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.
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.

Variable	Value
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.

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.

Attention: 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 (page 47)
- Changing the IP multicast settings (page 48)
- Disconnecting Terminal Services sessions (page 50)

Configuring the Multicast controller

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.

Prerequisites

- Ensure that you know the Administrator password.

Procedure steps

Step	Action
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.

Attention: 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.

Attention: 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**.

--End--

Changing the IP multicast settings

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.

Prerequisites

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

Procedure steps

Step	Action
1	On the Contact Center Manager Server, click **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**.

--End--

Variable definitions

Variable	Value
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

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.

Prerequisites

- Plan to use unicast transmission for statistics.

Procedure steps

Step	Action
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.

--End--

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 (page 52)
- Configuring the system data source names (page 53)
- Configuring HDX and TAPI server settings (page 55)
- Configuring the database connections (page 58)
- Configuring Web services (page 59)
- Removing a Web service package (page 60)
- Constructing and testing SQL statements or stored procedures (page 61)
- Updating an SQL statement (page 62)
- Deleting an existing SQL statement or stored procedure (page 62)
- Configuring the Contact Center Manager Server script (page 63)
- Backing up the Database Integration Service (page 64)
- Restoring the configuration (page 65)

Creating and invoking a stored procedure

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 steps

Step	Action
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.

--End--

Example of creating and invoking a stored procedure

Step	Action
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
```

--End--

Configuring the system data source names

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.

Prerequisites

- 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.

Procedure steps

Step	Action
1	Open Windows Explorer.
2	Browse to the following folder location 'C:\Windows\SysWOW64, to launch the 32-bit version of the ODBC Data Source Administrator.

Attention: 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.

Attention: Check the version of Sybase ASE ODBC Driver under the Drivers tab. The version should 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.

--End--

Configuring HDX and TAPI server settings

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.

Prerequisites

- 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 (page 53)
- 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.

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

Procedure steps

Step	Action
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.
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.

Attention: 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.

Attention: 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**.

Attention: 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**, click **Next**.

16 On the **Complete** window, click **Finish** to accept the changes and close the wizard.

--End--

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

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

Prerequisites

- 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.

Procedure steps

Step	Action
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.

Attention: 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**.

Attention: 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.

--End--

Configuring Web services

Configure Web services to import Web service functionality.

Attention: 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.

Prerequisites

- 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 4.

Procedure steps

Step	Action
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**.

Attention: 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**.

--End--

Removing a Web service package

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

Procedure steps

Step	Action
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.

--End--

Constructing and testing SQL statements or stored procedures

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.

Prerequisites

- 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.

Procedure steps

Step	Action
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.

--End--

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

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

Procedure steps

Step	Action
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.

--End--

Deleting an existing SQL statement or stored procedure

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

Procedure steps

Step	Action
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.

--End--

Configuring the Contact Center Manager Server script

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.

Prerequisites

- 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.

Procedure steps

Step	Action
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.

--End--

Backing up the Database Integration Service

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.

Prerequisites

- 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.

Procedure steps

Step	Action
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.

--End--

Restoring the configuration

Restore the configuration from a previous backup.

Prerequisites

- 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.

Procedure steps

Step	Action
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**.

--End--

Contact Center Manager Server Utility

- Access Class operations (page 69)
- Connected user and user account operations (page 75)
- Serial port configuration (page 91)
- Server settings (page 95)
- PABX configuration (page 97)
- Alarm and Event configuration (page 99)
- Provider configuration (page 113)
- PC Event Browser configuration (page 115)
- Contact Center Service Monitor configuration (page 117)
- Voice Prompt Editor configuration (page 121)

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 (page 70)
- Creating an access class (page 70)
- Viewing members of an access class (page 71)
- Modifying access class properties (page 72)
- Previewing the list of access classes (page 73)
- Printing the list of access classes (page 73)
- Deleting an access class (page 74)

Logging on to Server Utility

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

The default login information for the Server Utility is

- User ID: sysadmin
- Password: avaya1

Procedure steps

Step	Action
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**.

--End--

Creating an access class

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.

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 70).

Procedure steps

Step	Action
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 and step 8 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**.

--End--

Viewing members of an access class

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

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 70).

Procedure steps

Step	Action
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**.

--End--

Modifying access class properties

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.

Prerequisites

- Log on to Server Utility as a system administrator. See Logging on to Server Utility (page 70).
- Create the access classes to modify. See Creating an access class (page 70).
- Configure users in CCMA. See *Avaya Aura™ Contact Center Manager Administration – Client Administration* (NN44400-611).

Procedure steps

Step	Action
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 and step 9 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**.

--End--

Previewing the list of access classes

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

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 70).

Procedure steps

Step	Action
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.*

--End--

Variable definitions

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

Printing the list of access classes

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

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 70).

Procedure steps

Step	Action
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**.

--End--

Deleting an access class

Delete an access class that you no longer use.

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

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 70).

Procedure steps

Step	Action
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**.

--End--

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 (page 70).

Navigation

- Viewing a list of connected users (page 76)
- Printing a list of connected users (page 76)
- Logging off a user (page 77)
- Setting privileges for a user (page 77)
- Adding desktop user accounts (page 84)
- Preventing users from accessing the server (page 85)
- Restoring access to the server for a user (page 85)
- Resetting desktop passwords (page 86)
- Changing the properties of a desktop user (page 88)
- Printing a list of users (page 88)
- Deleting a desktop user (page 89)

Viewing a list of connected users

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

Procedure steps

Step	Action
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**.

--End--

Printing a list of connected users

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 steps

Step	Action
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**.

--End--

Logging off a user

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

Procedure steps

Step	Action
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**.

--End--

Setting privileges for a user

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

Procedure steps

Step	Action
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 (page 84)
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 (page 88)

--End--

Procedure job aid

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

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

(1 of 6)

Function	Privilege	Description
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.
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

Function	Privilege	Description
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.
	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.

Function	Privilege	Description
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.
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.

Function	Privilege	Description
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.
	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.

Function	Privilege	Description
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.
(6 of 6)		

Adding desktop user accounts

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

If adding a new desktop user account in a contact center that uses the High Availability feature it may take up to 6 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.

Prerequisites

- Create at least one access class. See Creating an access class (page 70)

Procedure steps

Step	Action
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. **Attention:** 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**.

--End--

Preventing users from accessing the server

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

Prerequisites

- Log off the desktop user. See Changing the properties of a desktop user (page 88).

Procedure steps

Step	Action
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**.

--End--

Restoring access to the server for a user

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 steps

Step	Action
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**.

--End--

Resetting desktop passwords

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.

Prerequisites

- Log on to Server Utility as sysadmin.

Procedure steps

Step	Action
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** window.
7	Click **Save**.
8	Click **File**, **Close**.

--End--

Changing the properties of a desktop user

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

Prerequisites

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

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

Procedure steps

Step	Action
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.

--End--

Printing a list of users

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

Procedure steps

Step	Action
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**.

--End--

Deleting a desktop user

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

Prerequisites

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

Attention: If the User is logged in it will be logged off without warning when it is deleted.

Procedure steps

Step	Action
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**.

--End--

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 (page 70).

Navigation

- Viewing port settings (page 92)
- Printing port settings (page 92)
- Editing port settings (page 93)

Viewing port settings

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

Procedure steps

Step	Action
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**.

--End--

Printing port settings

Print the port settings.

Procedure steps

Step	Action
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**.

--End--

Editing port settings

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 steps

Step	Action
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.

--End--

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 (page 70).

Navigation

- Viewing server resources (page 95)
- Printing server resources information (page 96)

Viewing server resources

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 steps

Step	Action
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**.

--End--

Printing server resources information

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

Procedure steps

Step	Action
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**.

--End--

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 (page 97)

Recording PABX information

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 steps

Step	Action
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**.

--End--

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 Event Browser versus Alarm Monitor features (page 100).

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 (page 70).

Navigation

- Starting the Event Browser (page 100)
- Starting the Event Browser from Server Utility (page 101)
- Sorting events in the Event Browser (page 102)
- Viewing online Help for an event (page 102)
- Saving a list of events (page 102)
- Printing a list of events (page 103)
- Changing the filtering criteria for events (page 104)
- Adding an event preference (page 105)
- Throttling all events (page 106)

- Changing an event preference (page 107)
- Printing the list of event preferences (page 107)
- Deleting an event preference (page 107)
- Changing the classification of an event (page 108)
- Opening the Alarm Monitor (page 108)
- Refreshing the Alarm Monitor (page 109)
- Sorting events in the Alarm Monitor (page 109)
- Specifying when the Alarm Monitor appears in the foreground (page 110)
- Configuring the Alarm Monitor to appear in the background (page 110)
- Obtaining more information about an alarm (page 111)
- Manually clearing an alarm (page 111)

Starting the Event Browser

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

Procedure steps

Step	Action
1	Click **Start, All Programs, Avaya, Contact Center, Server Utility, PC Event Browser**.

--End--

Procedure job aid

Event Browser versus Alarm Monitor features

Feature	In Event Browser?	In Alarm Monitor?
View events	Yes	Yes
View online Help for an event	Yes	Yes
Sort events by category	Yes	Yes
Save a list of events	Yes	No
Print a list of events	Yes	Yes
View minor, major, critical events	Yes	Yes
View information events	Yes	No

Event Browser versus Alarm Monitor features

Feature	In Event Browser?	In Alarm Monitor?
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

You can start the Event Browser from the Server Utility.

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 70).

Procedure steps

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

--End--

Sorting events in the Event Browser

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

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 101).

Procedure steps

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

--End--

Viewing online Help for an event

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.

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 101).

Procedure steps

Step	Action
1	In the Event Browser, double-click the event to you want to investigate.
2	Click **Help on Event**.

--End--

Saving a list of events

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.

Prerequisites

- Ensure the filter settings are configured to show the type and number of events to save. See Changing the filtering criteria for events (page 104).

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 101).

Procedure steps

Step	Action
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**.

--End--

Printing a list of events

Print a record of events for technical support.

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 101).

Procedure steps

Step	Action
1	On the Events Browser window, click **File, Print**.
2	Select the printer and printer options.
3	Click **OK**.

--End--

Changing the filtering criteria for events

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

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 101).

Procedure steps

Step	Action
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.

--End--

Adding an event preference

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.

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 101).

Procedure steps

Step	Action
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.

Attention: Contact Center Manager Server does not accept unrecognizable event codes. For a complete list of valid event codes, see to the Event Browser 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**.

--End--

Variable definitions

Variables	Value
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

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

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 101).

Procedure steps

Step	Action
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**.

--End--

Changing an event preference

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

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 101).

Procedure steps

Step	Action
1	From the Event Browser window, select the Event Preference to change.
2	Click **File**, **Event Details**.

--End--

Printing the list of event preferences

Print the list of event preferences for your records.

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 101).

Procedure steps

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

--End--

Deleting an event preference

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

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 101).

Procedure steps

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

--End--

Changing the classification of an event

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.

Prerequisites

- Open the Event Browser. See Starting the Event Browser from Server Utility (page 101).

Procedure steps

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

--End--

Opening the Alarm Monitor

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.

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 70).

Procedure steps

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

--End--

Refreshing the Alarm Monitor

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

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

Prerequisites

- Open the Alarm Monitor. See Opening the Alarm Monitor (page 108).

Procedure steps

Step	Action
1	From the Alarm Monitor window, click **View, Refresh**.

--End--

Sorting events in the Alarm Monitor

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

Prerequisites

- Open the Alarm Monitor. See Opening the Alarm Monitor (page 108).

Procedure steps

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

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

--End--

Specifying when the Alarm Monitor appears in the foreground

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.

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 70).

Procedure steps

Step	Action
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.

--End--

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

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.

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 70).

Procedure steps

Step	Action
1	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.*

--End--

Obtaining more information about an alarm

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

Prerequisites

- Open the Alarm Monitor. See Opening the Alarm Monitor (page 108).

Procedure steps

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

--End--

Manually clearing an alarm

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.

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

Prerequisites

- Open the Alarm Monitor. See Opening the Alarm Monitor (page 108).

Procedure steps

Step	Action
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 to clear the selected alarm.

--End--

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 (page 113)
- Connecting to the Contact Center Manager Server (page 113)

Starting the Provider

Start the Provider to receive Contact Center scripts.

Prerequisites

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

Procedure steps

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

--End--

Connecting to the Contact Center Manager Server

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.

Prerequisites

- 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 (page 113).

Procedure steps

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

--End--

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 (page 115)

Starting the PC Event Browser

Start PC Event Browser.

Procedure steps

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

--End--

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 (page 118)
- Changing the site to monitor (page 119)
- Exiting Networking Service Monitor (page 119)
- Refreshing the service status (page 119)
- Configuring the default site information (page 120)

Starting Contact Center Service Monitor

Start Contact Center Service Monitor.

Procedure steps

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

--End--

Changing the site to monitor

Monitor the service status of other servers in the network.

Prerequisites

- Start Contact Center Service Monitor. See Starting Contact Center Service Monitor (page 118).

Procedure steps

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

--End--

Exiting Networking Service Monitor

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

Prerequisites

- Start Contact Center Service Monitor. See Starting Contact Center Service Monitor (page 118).

Procedure steps

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

--End--

Refreshing the service status

Refresh the status of services.

Prerequisites

- Launch Contact Center Service Monitor. See Starting Contact Center Service Monitor (page 118).

Procedure steps

Step	Action
1	Click **Refresh Service Status**.

--End--

Configuring the default site information

Configure the default monitored site.

Prerequisites

- Start Contact Center Service Monitor. See Starting Contact Center Service Monitor (page 118).

Procedure steps

Step	Action
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.

--End--

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 (page 122)
- Logging off the Voice Prompt Editor (page 122)
- Creating a voice file (page 123)
- Opening a voice file (page 123)
- Reverting to a previously saved voice file (page 124)
- Copying a voice file (page 124)
- Renaming a voice file (page 124)
- Deleting a voice file (page 125)
- Restoring a voice file (page 125)
- Creating a voice segment (page 126)
- Recording a voice segment (page 126)
- Playing a voice segment (page 127)
- Playing a group of voice segments (page 128)
- Searching for a voice segment (page 128)
- Lengthening or shortening a voice segment (page 129)
- Removing all silence from a voice segment (page 130)
- Removing or adding a specified length to all voice segments (page 131)
- Removing all silence from all voice segments (page 132)
- Deleting a voice segment (page 133)
- Restoring a voice segment marked for deletion (page 133)

Logging on to the Voice Prompt Editor

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

Prerequisites

- Log on to Server Utility. See Logging on to Server Utility (page 70).

Procedure steps

Step	Action
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**.

--End--

Logging off the Voice Prompt Editor

Exit the Voice Prompt Editor.

Prerequisites

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

Procedure steps

Step	Action
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**.

--End--

Creating a voice file

Organize your voice segments into a voice file.

Prerequisites

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

Procedure steps

Step	Action
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**.

--End--

Opening a voice file

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

Prerequisites

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

Procedure steps

Step	Action
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.*

--End--

Reverting to a previously saved voice file

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.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 122).
- Open a voice file and make changes to it. See Opening a voice file (page 123).

Procedure steps

Step	Action
1	From the **Voice Prompt Editor** window, choose **File**, **Revert**.

--End--

Copying a voice file

Copy a voice file.

Prerequisites

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

Procedure steps

Step	Action
1	From the **Voice Prompt Editor** window, choose **File**, **Copy**.

--End--

Renaming a voice file

Rename a voice file.

Prerequisites

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

Procedure steps

Step	Action
1	From the **Voice Prompt Editor** window, choose **File**, **Rename**.

--End--

Deleting a voice file

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.

Prerequisites

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

Procedure steps

Step	Action
1	From the **Voice Prompt Editor** window, choose **File**, **Delete**.

--End--

Restoring a voice file

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.

Prerequisites

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

Procedure steps

Step	Action
1	From the **Voice Prompt Editor** window, choose **File**, **Undelete**.

--End--

Creating a voice segment

Create voice segments to add to voice files.

Prerequisites

- Log on to the Voice Prompt Editor. See Logging on to the Voice Prompt Editor (page 122).
- Open a voice file. See Opening a voice file (page 123).

Procedure steps

Step	Action
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.*

--End--

Recording a voice segment

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

Prerequisites

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

Procedure steps

Step	Action
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, say the words that you want to record in the voice segment.
5	Click the **Stop** icon.

6 Hang up.

7 To record another segment, repeat step 2 to step 6.

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

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

--End--

Playing a voice segment

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

Prerequisites

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

Procedure steps

Step	Action
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 backward increments of 5 seconds, click the **Skip Backward** icon. **OR** To move forward by increments of 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.

--End--

Playing a group of voice segments

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.

Prerequisites

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

Procedure steps

Step	Action
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 to step 3 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.

--End--

Searching for a voice segment

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

Prerequisites

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

Procedure steps

Step	Action
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.

--End--

Lengthening or shortening a voice segment

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

Prerequisites

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

Procedure steps

Step	Action
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.

--End--

Removing all silence from a voice segment

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.

Prerequisites

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

Procedure steps

Step	Action
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.*

--End--

Removing or adding a specified length to all voice segments

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

Prerequisites

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

Procedure steps

Step	Action
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.

--End--

Removing all silence from all voice segments

Remove all silence from all voice segments at one time.

Prerequisites

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

Procedure steps

Step	Action
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.

--End--

Deleting a voice segment

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.

Prerequisites

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

Procedure steps

Step	Action
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.*

--End--

Restoring a voice segment marked for deletion

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.

Prerequisites

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

Procedure steps

Step	Action
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.*

--End--

Contact Center Manager Administration

- Contact Center Manager Administration configuration (page 137)
- Avaya Communication Server 1000 Data Extraction Tool operation (page 163)
- Active Directory Lightweight Directory Services replication (page 187)
- CCMA and Security Framework backup and restore (page 173)
- Contact Center Manager Administration failure recovery (page 193)
- Language support fundamentals (page 197)
- Language support configuration (page 203)
- Security Framework configuration (page 201)

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 (page 138)
- Configuring your logon warning message title and text (page 139)
- Enabling the logon warning message (page 140)
- Configuring Real-Time Reporting (page 141)
- Configuring Emergency Help (page 143)
- Configuring e-mail notifications for Historical reporting (page 144)
- Configuring SMTP Server on the Contact Center Manager Administration (page 146)
- Creating a shared folder to export historical reports (page 147)
- Installing the Service Creation Environment (page 149)
- Configuring Agent Desktop Display parameters on the server (page 150)
- Changing the password for the iceAdmin user account (page 153)
- Configuring the LPR port for printers (page 154)
- Configuring a network printer on the CCMA server (page 154)
- Configuring a network printer to use the CCMA server as the print server (page 156)

- Configuring a network printer to use a print server other than the CCMA server (page 157)
- Installing the XML Automated Assignments feature (page 158)
- Configuring Avaya Call Recording and Quality Monitoring (page 159)
- Configuring CDN Landing Pads for Universal Networking or Integrated Reporting (page 160)
- Configuring a DNIS Landing Pad for Universal Networking (page 161)

Configuring the Contact Center License Manager Service

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.

Prerequisites

- 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.

Procedure steps

Step	Action
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.

--End--

Configuring your logon warning message title and text

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, a 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.

Prerequisites

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

Procedure steps

Step	Action
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.

--End--

Enabling the logon warning message

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 (page 141).

Prerequisites

- 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 (page 139).

Procedure steps

Step	Action
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 **LoginWarning 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.

--End--

Configuring Real-Time Reporting

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.

Prerequisites

- 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.

Procedure steps

Step	Action
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).

Attention: 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.

Attention: 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.

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.

--End--

Variable definitions

Variable	Value
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

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.

Prerequisites

- 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.

Procedure steps

Step	Action
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.

--End--

Configuring e-mail notifications for Historical reporting

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.

Prerequisites

- 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).

Procedure steps

Step	Action
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 (page 146)
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.
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**.

--End--

Variable definitions

Variable	Value
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

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.

Prerequisites

- 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).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Click **Start**, **Administrative Tools**, **Internet Information Services (IIS) Manager**.
3	In the left pane of the **Internet Information Services (IIS) Manager** window, expand **<Computer Name> (local computer)**.
4	Right-click the **Default SMTP Virtual Server**, 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.

--End--

Variable definitions

Variable	Value
<Computer Name> (local computer)	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

Create a shared folder to export historical reports if you want multiple users to access scheduled historical reports from the same folder.

Prerequisites

- Grant change and read permissions to the users who can access the scheduled report account; for example, the iceAdmin account or the domain account.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Create a folder.
3	Right-click the new folder and select **Sharing and Security**.
4	In the **<folder name> Properties** dialog box, on the **Sharing** page, select the **Share this folder** option.
5	Click **Permissions**.
6	In the **Permissions for <folder name>** dialog box, in the **Groups or user names** list, select **Everyone**.
7	To grant change and read permissions to the Everyone account, proceed to step 16.
8	To grant change and read permissions to the iceAdmin or domain account, click **Remove** to remove the **Everyone** account.
9	Click **Add**.
10	In the **Select Users, Computers, or Groups** dialog box, click **Advanced**.
11	Click **Find Now**.
12	In the expanded portion of the **Select Users or Groups** dialog box, locate and select the **iceAdmin** account **OR** Select the domain account used for IIS directory security.
13	Click **OK**.
14	In the **Select Users, Computers, or Groups** dialog box, click **OK**.
15	In the **Permissions** dialog box, select the account that you selected in step 12.
16	Select the **Allow** check box for the following: • Change • Read
17	Click **Apply**.
18	Click **OK** to close the **Permissions for <folder name>** dialog box.
19	Click **Apply**.
20	Click **OK** to close the **<folder name> Properties** dialog box.

--End--

Installing the Service Creation Environment

Install the Service Creation Environment 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 steps

Step	Action
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 **Service Creation**, and then click **Launch Service Creation**.
4	In the message box requesting you to download a .msi file, click **OK**.
5	In the dialog box, click **Run**.
6	In the **Service Creation Environment - 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 folder is where the offline application is installed.
12	Click **Next**.
13	Click **Install**.
14	Click **Finish**.

--End--

Procedure job aid

Information about the Service Creation Environment is found in *Avaya Aura™ Contact Center Configuration – Service Creation Environment Application Development* (NN44400-510).

Configuring Agent Desktop Display parameters on the server

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 Display 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 Display to function properly.

Prerequisites

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

Procedure steps

Step	Action
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 Display 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 Display, select the **Agents phoneset login required for ADD** check box.
7	To disable automatic notifications for Agent Desktop Display 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 Display.
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 Display when the value reaches the threshold, select the **Blink** check box.

13 If you want the Agent Desktop Display 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.

14 To indicate that a beep should occur only once, select the **Once** option.

OR

To indicate that a beep should occur continuously until the statistic reaches an acceptable value, select **Continuously**.

15 Click **Save**.

--End--

Variable definitions

Variable	Value
Agents phoneset login required for Agent Desktop Display	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 Display, the agent sees data only if other agents log on to skillsets to which that agent is assigned.
IP multicast address	The IP multicast addresses that you select for RSM sending and receiving must be within the 224.0.1.0 and 239.255.255.255 range. Check with your network administrator for acceptable IP multicast addresses for your specific network.
Max agents	The maximum number of agents who can simultaneously log on to the Agent Desktop Display 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 3 000 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

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 (page 536).

Prerequisites

- 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.

Procedure steps

Step	Action
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.
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.

Attention: 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**.

--End--

Configuring the LPR port for printers

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

Prerequisites

- Ensure that you have the Windows Server 2008 Release 2 installation disk.

Procedure steps

Step	Action
1	Log on to the server.
2	Click **Start, Administrative Tools, Server Manager.**
3	In the **Server Manager** window, right-click **Roles** and select **Add Roles**.
4	Click **Next**.
5	Select the **File Services** check box and click **Next**.
6	On the **File Services** page, click **Services for Network File System** and click **Next**.
7	Click **Install**.
8	Click **Close**.

--End--

Configuring a network printer on the CCMA server

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.

Prerequisites

- 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.

Procedure steps

Step	Action
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, Printers and Faxes**.
9	In the **Printers and Faxes** window, double-click **Add a printer**.
10	In the **Add Printer Wizard**, click **Next**.
11	In the **Local or Network Printer** dialog box, select the **Local printer attached to this computer** option.
12	Clear the **Automatically detect and install my Plug and Play printer** check box.
13	Click **Next**.
14	In the **Select the Printer Port** dialog box, select the **Use the following port** option.
15	From the list, select the port you typed in step 5.
16	Click **Next**.
17	In the **Install Printer Software** dialog box, in the **Manufacturer** and **Printers** lists, select the appropriate information for your printer.
18	Click **Next**.
19	In the **Name your printer** dialog box, for the question **Do you want to use this printer as the default printer**, select **Yes**.
20	Click **Next**.
21	In the **Printer Sharing** dialog box, select **Do not share this printer**.
22	Click **Next**.
23	In the **Print Test Page** dialog box, for the question **Do you want to print a test page**, select **No**.
24	Click **Next**.
25	In the **Completing the Add Printer Wizard** dialog box, click **Finish**.

--End--

Variable definitions

Variable	Value
<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

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

Prerequisites

- 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.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Click **Start, Printers and Faxes**.
3	In the **Printers and Faxes** window, double-click **Add a printer**.
4	In the **Add Printer Wizard**, click **Next**.
5	In the **Local or Network Printer** dialog box, select the **Local printer attached to this computer** option.
6	Clear the **Automatically detect and install my Plug and Play printer** check box.
7	Click **Next**.
8	Select the **Create a new port** option.
9	From the **Type of port** list, select **Standard TCP/IP Port**.
10	Click **Next**.
11	In the **Welcome to the Add Standard TCP/IP Printer Port Wizard** dialog box, click **Next**.
12	In the **Add Port window** dialog box, in the **Printer Name or IP address** box, type the printer IP address.
13	Click **Next**.

14 In the **Completing the Add Standard TCP/IP Printer Port Wizard** dialog box, click **Finish**.

15 In the **Install Printer Software** dialog box, in the **Manufacturer** and **Printer** boxes, select the appropriate information for your printer.

16 Click **Next**.

17 In the **Name Your Printer** dialog box, type the printer name (or accept the default name).

18 Click **Next**.

19 In the **Printer Sharing** dialog box, accept the default with **Share name** selected.

20 Click **Next**.

21 (Optional) In the **Location and Comment** dialog box, in the **Location and Comment** boxes, type location and comment information.

22 Click **Next**.

23 In the **Print Test Page** dialog box, click **Yes** to print a test page.

24 In the **Completing the Add Printer Wizard** dialog box, click **Finish**.

--End--

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

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).

Prerequisites

- 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.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Click **Start, Printers and Faxes**.
3	In the **Printers and Faxes** window, double-click **Add a printer**.
4	In the **Add Printer Wizard**, click **Next**.

5	In the **Local or Network Printer** dialog box, select **Local printer attached to this computer**.
6	Clear the **Automatically detect and install my Plug and Play printer** check box.
7	Click **Next**.
8	Select **Create a new port**.
9	From the **Type of port** list, select **LPR port**.
10	Click **Next**.
11	In the **Add LPR Compatible Printer** dialog box, in the **Name or address of server providing lpd** box, type the Domain Name Service (DNS) name or IP address of the print server.
12	In the **Name of printer or print queue on that server** box, type the name of the printer as it is identified by the host, which is either the direct-connect printer or the UNIX computer.
13	Click **OK** to close the window and return to the wizard.
14	Follow the remaining prompts in the wizard to finish installing the printer.

--End--

Installing the XML Automated Assignments feature

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.

Prerequisites

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

Procedure steps

Step	Action
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 error. 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**.

--End--

Configuring Avaya Call Recording and Quality Monitoring

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 steps

Step	Action
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 which 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 which runs on the Quality Archiver server.

19 Click **Submit** to save the changes.

--End--

Configuring CDN Landing Pads for Universal Networking or Integrated Reporting

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 will be routed to an agent. For Integrated Reporting, the call will be 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 only supported 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.

Prerequisites

Configure the CDNs on the telephony PABX. For information about configuring a CDN on the telephony PABX, see Contact Center *Configuration* – Avaya Communication Server 1000 *Integration (NN44400-512)*.

Procedure steps

Step	Action
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.

--End--

Configuring a DNIS Landing Pad for Universal Networking

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 will be 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.

Prerequisites

Configure the DNISs on the telephony PABX. For information about configuring the telephony PABX, see Contact Center *Configuration* – Avaya Communication Server 1000 *Integration (NN44400-512)*.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration.
2	On the launch pad, click **Configuration**.
3	In the left pane, expand the server under which to add the DNIS LandingPad.
4	Click the **DNISs** 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.

--End--

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 (page 164)
- Extracting data using a modem (page 165)
- Extracting data from a file (page 166)
- Capturing Terminal Number data (page 167)
- Capturing voice port data (page 169)
- Capturing CDN data (page 169)
- Capturing IVR ACD-DN data (page 170)
- Capturing route data (page 171)

Extracting data from a serial connection

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.

Prerequisites

- 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.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, Contact Center, **CS100 Data Extraction Tool**, **CS 1000 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.

Attention: 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.

--End--

Extracting data using a modem

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

Prerequisites

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

Procedure steps

Step	Action
1	From the **Start** menu, select **Programs**, select Contact Center, select **CS100 Data Extraction Tool**, and then click **CS 1000 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 & Supervisor 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.

--End--

Extracting data from a file

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.

Prerequisites

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

Procedure steps

Step	Action
1	From the **Start** menu, point to **Programs**, point to Contact Center, point to **CS100 Data Extraction Tool**, and then click **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.

--End--

Capturing Terminal Number data

Capture a list of all configured Terminal Numbers (TNs).

Prerequisites

- Connect to Overlay program 20.

Procedure steps

Step	Action
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.

--End--

Example of capturing terminal data

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

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.

Prerequisites

- Log onto Overlay program 81.

Procedure steps

Step	Action
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**

--End--

Output example

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

You can capture a list of all of the CDNs by using Overlay program 23.

Prerequisites

- Connect to Overlay 23.

Procedure steps

Step	Action
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**

--End--

Example of Overlay 23 output

```
TYPE CDN
CUST 0
CDN 4911
FRRT
SRRT
....
ACNT
```

Capturing IVR ACD-DN data

Capture a list of all of the IVR ACD-DNs by using Overlay program 23.

Prerequisites

- Connect to Overlay 23.

Procedure steps

Step	Action
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.

--End--

Example of output from option 11C for IVR ACD-DNs

```
TYPE ACD
CUST 0
ACDN 6700
....
CWNT NONE
```

Capturing route data

Capture a list of all of the route numbers from the PABX by using Overlay program 21.

Prerequisites

- Connect to Overlay program 21.

Procedure steps

Step	Action
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.

--End--

CCMA and Security Framework backup and restore

Avaya recommends that all contact centers perform regular backups of Contact Center Manager Administration data files to a secure location such as a network drive. You can help your contact center to recover from events, such as data loss and damage due to disk failures and power outages, by creating a backup of your contact center data. This applies to data on the Contact Center Manager Administration server and on the server in Contact Center Manager Server. This can be the same server if you work on a co-resident installation.

If you install a replicating server, you must perform regular backups of the active Contact Center Manager Administration server. Unlike Microsoft Active Directory Lightweight Directory Services (AD-LDS) replication, backups provide snapshots of your Contact Center Manager Administration data files at moments in time. Backing up data and not using AD-LDS replication as the only method of backing up Contact Center Manager Administration data is important for the following two reasons:

- Not all Contact Center Manager Administration data is stored in AD-LDS and therefore is not replicated.
- You cannot use replication to roll back data to a specific time, which may be required.

You can use the Backup and Restore utility to back up a preselected series of Contact Center Manager Administration files (including Historical Reporting files, AD-LDS files, and database files). You can also use the utility to schedule singular or multiple backup tasks on a daily, weekly, or monthly basis. However, you cannot use this utility to back up operating system files or data files that are not related to Contact Center Manager Administration.

In addition to backing up files, you must record your Real-Time Reporting configuration settings and your Emergency Help configuration settings whenever these settings change. During the restoration, you must manually reconfigure these settings.

You must back up Contact Center Manager Administration data for the following reasons:

- To avoid loss of data in the event of a server failure, Avaya recommends that you schedule backups and back up your Contact Center Manager Administration data at least once a day (or more frequently based on your contact center requirements). Schedule backups during periods of low activity.
- If you upgrade Contact Center Manager Administration or if you migrate Contact Center Manager Administration to a new server, you must perform a full backup of your Contact Center Manager Administration before you perform the update or migration.

- To keep data synchronized between Contact Center Manager Administration and Contact Center Manager Server, you must back up and restore Contact Center Manager Administration data and your Contact Center Manager Server data at the same time to ensure proper functionality in your contact center. If the Contact Center Manager Server files change infrequently, you can back up only the Contact Center Manager Administration data. In a co-resident environment, when you perform a full backup of Contact Center Manager Server, you back up the entire server, including Contact Center Manager Administration. This ensures that the data between the two applications is always synchronized. However, whenever you perform a partial backup of Contact Center Manager Server, you must also perform a backup of Contact Center Manager Administration. Furthermore, you must store both backups in the same location.

Having current backup data is essential:

- to revert back to a previous version of the software, if necessary, following an upgrade
- to migrate Contact Center Manager Administration data to a new server
- to roll back erroneous data
- to recover from catastrophic events (such as data loss and damage due to disk failures and power outages)

You also can back up and restore the Security Framework in the same method as you use to back up the Contact Center Manager Administration server.

Prerequisites

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

Navigation

- Backing up Contact Center Manager Administration (page 175)
- Backing up Security Framework (page 179)
- Viewing scheduled tasks in the Backup and Restore utility (page 181)
- Recording Real-Time Reporting and Emergency Help configurations (page 182)
- Restoring Contact Center Manager Administration data (page 182)
- Restoring Security Framework data (page 185)
- Switching to the standby server in Agent Desktop Display (page 186)

Backing up Contact Center Manager Administration

Back up Contact Center Manager Administration to a folder to create a snapshot of the preselected CCMA files. You can create the folder location on the same server or on another domain server.

The Backup and Restore utility is automatically installed on the CCMA server when you install the CCMA software.

You use this utility to back up the files located in the following folders (where C is the drive on which you installed CCMA):

- AD-LDS-specific data stored in the following folder:
  C:\Program Files (x86)\Microsoft ADAM\
- Historical reporting template files (both imported and custom) and Audit Trail event logs stored in the following folders:
  D:\Avaya\Contact Center\Manager Administration\Apps\Reporting\
  D:\Avaya\Contact Center\Manager Administration\Apps\Common\
- The Report Creation Wizard database files stored in the following folder:
  D:\Avaya\Contact Center\Manager Administration\Server\RCW\Data
- A record of displays for real-time reporting exported to the following folder:
  D:\Avaya\Contact Center\Manager Administration\Apps\Reporting\
- An index file for Custom Report Groups stored in the following folder:
  D:\Avaya\Contact Center\Manager Administration\Apps\AccessMgt\
- A record of displays for Emergency Help exported to the following folder:
  D:\Avaya\Contact Center\Manager Administration\Apps\EmergencyHelp\

Prerequisites

- Install the Windows Server 2008 - Windows Server Backup utility on the Contact Center Manager Administration server.
- Ensure that you have write privileges on the server where you want to store the CCMA data you are backing up.
- Log on to the CCMA server with administrative privileges.

Attention: The Backup and Restore Utility supports only NTFS-formatted drives (either local drives or network locations). If you attempt to create a backup on a FAT32-formatted drive, the backup will fail.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, click **Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration**.
2	In the left pane of the Configuration window, expand **Avaya**, **Applications**.
3	In the **Avaya Applications Configuration** window, select **Backup & Restore**.
4	In the right-hand pane, click **Backup & Restore**.
5	In the **Contact Center Manager Administration - Backup and Restore** utility, select the **Backup** tab.
6	In the **Backup** window, select the **Drive** or specify the **Network Location** where you want to store the backup.
7	Click **Next**.
8	On the **Schedule** page, select an option to schedule the backups.
9	Define the backup schedule, and then click **Next**.
10	In the **Username** box on the **User Account with Administrative Privileges** page, type a valid administrator user name for the server on which you want to store the backup.
11	In the **Password** box, type a the password for the specified administrator user.
12	If you selected a backup location on another server in a domain, type the domain in the **Domain** field. The default option is **this computer** (that is, the Contact Center Manager Administration server on which you are creating the backup).
13	Click **Finish**.
14	Click **Close**.

--End--

Variable definitions

Variable	Value
Drive	The local hard drive where you would like to store the backup. The Backup and Restore Utility supports only NTFS-formatted drives (either local drives or network locations). If you attempt to create a backup on a FAT32-formatted drive, the backup will fail. This list shows available local hard drives and any network drives mapped on the server. Note that any drives included in the backup (typically C: and D:) do not appear in the list: these are not supported by the backup application. DVD drives do not appear in the list.
Network Location	The network location where you want to store the backup, in UNC format \\Computer Name\Folder.
Schedule options	The time interval for scheduled backups. This can be • Daily (to schedule recurring backups once a day) • Weekly (to schedule recurring backups once a week) • Monthly (to schedule recurring backups once a month) • One Time Only (to schedule a one-time-only backup at a time in the future) • Run Now (to back up files immediately after you enter a valid username and password) If you select Monthly, you can schedule a task only on the last day of the month that contains the least number of days. For example, if you want the backup to run every month, then you can schedule it to occur on day 28 only. However, if you clear February from the schedule, then the last possible day of a monthly schedule is 30. If you clear April, June, September, and November from the schedule, then the last possible day of a monthly schedule is 31.

Variable	Value
Username and Password	You must configure a user name and password with write privileges on the server on which you want to store the backup.
Domain	If you selected a backup location on another server, type that server's domain. The username and password must be valid on this domain and have administrative privileges on the server specified in Network Location.

Procedure job aid

Data files stored on Contact Center servers

Contact Center server	Data files stored on server	Business consequence of CCMA server failure
Contact Center Manager Administration server	Schedule information for historical reports Partitions, access classes, report groups, and the Contact Center Manager Administration users Real-time display configuration data and real-time display filters Private historical reports Contact CenterManagement scheduled assignment information	If the Contact Center Manager Administration server fails, your supervisors and administrators cannot access the Contact Center Manager Administration application. Therefore, access to real-time displays, agent desktop display, schedule information for historical reports, and all data stored on in the application is interrupted.
Contact Center Manager Server	Agents, supervisors, skillsets and all their related assignments (accessed through Contact Center Management) CDNs, DNISs and all other data items (accessed through the Configuration component)	If your stand-alone Contact Center Manager Administration server fails, calls continue to be routed according to your defined scripts and your contact center can still receive calls because all user and agent assignments, CDNs, and DNISs are stored on the Contact Center Manager Server.

Backing up Security Framework

Back up the Security Framework data files to save a single file that is a snapshot of the Security Framework files. Save the backup file to a predefined location on the same server or on another server in the same domain.

The Backup and Restore utility for the Security Framework is automatically installed on the server when you install the Security Framework software.

When you back up the files with this utility, the system creates a single file that you can then use to restore the individual files. By default, this file is called Restore.bkf and is in the same folder.

Prerequisites

- Map a drive to the server in the domain where you want to back up Security Framework.
- Ensure that the Avaya JBoss and Avaya Common Network Directory services are running.
- Ensure that you have a user name and password configured with administrative privileges on the server where you want to back up Security Framework.

Procedure steps

Step	Action
1	On the Security Framework server, click **Start, All Programs, Avaya, Contact Center, Security Framework, Backup and Restore**.
2	In the **Security Framework - Backup and Restore** utility, select the **Backup** tab.
3	In the **Backup** window, select **File**.
4	Accept or change the location of the backup file, Restore.bkf.
5	From the **Archive Backup Files Every** list, select the number of backup files to keep in the backup location.
6	Click **Next**.
7	On the **Schedule** page, select an option to schedule the backups.
8	Define the backup schedule, and then click **Next**.
9	In the **Username** box on the **User Account with Administrative Privileges** page, type a valid administrator user name.
10	In the **Password** box, type a valid administrator password.
11	If you selected a backup location on another server in a domain, from the **Domain** list, select the domain.
12	Click **Finish**.
13	Click **Close**.

--End--

Variable definitions

Variable	Value
Archive Backup Files Every	You can keep 2 to 10 backups, or all backups. This provides the flexibility to retain only the most recent backups, to save space in your backup location.
Backup file name	This is the file that the utility creates when you back up the files. The file contains a snapshot of all Security Framework files that you back up. To change the default name or location of this file, click Browse, navigate to the location in which you want to store the file, and type a new file name. Avaya recommends that you change the name of the backup file from Restore.bkf to SF_7_[SPxx]_Restore.bkf where [SPxx] is replaced with the last Service Pack installed. To select a file location on another server in the domain, you must map a drive to that server and you must have read/write privileges on that server.
Schedule definition	You can schedule a task only on the last day of the month that contains the least number of days. For example, if you want the backup to run every month, then you can schedule it to occur on day 28 only. However, if you clear February from the schedule, then the last day of a monthly schedule is 30. If you clear April, June, September, and November from the schedule, then the last day of a monthly schedule is 31.

Variable	Value
Schedule options	The time interval for scheduled backups. This can be • Daily (to schedule recurring backups once a day) • Weekly (to schedule recurring backups once a week) • Monthly (to schedule recurring backups once a month) • One Time Only (to schedule a one-time-only backup at a time in the future) • Run Now (to back up files immediately after you enter a valid username and password)
Username and Password	You must configure a user name and password with administrative privileges on the server to which you back up.

Viewing scheduled tasks in the Backup and Restore utility

Use the Backup and Restore utility to view scheduled tasks, including the task status or scheduled run time, to review or delete scheduled tasks.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, click **Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration**.
2	In the left pane of the **Avaya Configuration** window, expand **Avaya** and **Administration**.
3	In the **Avaya Applications Configuration** window, click **Backup & Restore**.
4	In the right-hand pane, click **Backup & Restore**.
5	On the **Backup and Restore** utility, select the **View Scheduled Tasks** tab to display a list of scheduled tasks including the status and the next scheduled run time of each task.
6	To view the details of a task, highlight a task, and click **View Details** to display a detailed log file of your task.
7	To delete a task, highlight a task and click **Delete Task**.
8	On the confirmation box, click **Yes** to delete the task.
9	Click **Close**.

--End--

Recording Real-Time Reporting and Emergency Help configurations

Record the Real-Time Reporting configuration settings (IP Send and IP Receive Addresses) and the Emergency Help configuration settings whenever these settings change (for example, after you install or upgrade Contact Center Manager Administration).

Because these settings change infrequently and you cannot back them up using backup procedures, you must manually reconfigure the settings during a restoration.

Procedure steps

Step	Action
1	Click **Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration**.
2	In the left pane of the Configuration window, select the **Real-Time Reporting** folder.
3	In the right pane, select the **RTR Registry Settings** icon.
4	Record all settings in the **RTR Registry Settings** dialog box.
5	Close the **RTR Registry Settings** dialog box.
6	In the left pane of the **Configuration** window, select the **Emergency Help** folder.
7	In the right pane, select the **Emergency Help Registry Settings** icon.
8	Record all settings in the **Emergency Help Properties** dialog box.
9	Close all windows to complete the procedure.

--End--

Restoring Contact Center Manager Administration data

Restore Contact Center Manager Administration data in the following situations:

- if you recover from a Contact Center Manager Administration server hardware failure when Contact Center Manager Server data is being restored.
- if you move to a replicating server as a result of a failure on your primary Contact Center Manager Administration server.
- if you revert the Contact Center Manager Administration software to a previous version. You must restore data to the same version of Contact Center Manager Administration as you backed up.

- if you lose data or make an error while entering Contact Center Manager Administration data and you need a previous version of the data (Contact Center Manager Administration data is all data excluding configuration data, scripts, and agents and supervisors).
- if you migrate Contact Center Manager Administration data to a new server.

When you back up Contact Center Manager Administration data with the Backup and Restore utility, it creates a single file with the default name of Restore.bkf. If you need to restore the Contact Center Manager Administration data to the original state when you backed up the files, you can start the utility and navigate to this file.

Use the Backup and Restore utility to restore the series of specified Contact Center Manager Administration files that you backed up with this utility.

Prerequisites

- The Windows Server 2008 - Windows Server Backup utility must be installed on the Contact Center Manager Administration server.
- Restore data that was backed up from the same release and version of the software as 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.
- Retain the permission properties of the AD-LDS data directory and AD-LDS files if you restore these files (for example, you must retain permissions such as NETWORK SERVICE). If you do not maintain permission properties, the SymposiumWC service does not start.
- Restore the Contact Center Manager Administration data whenever you restore the Contact Center Manager Server data to prevent synchronization issues.
- The restore automatically reactivates scheduled events on the server.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, click **Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration**.
2	In the left pane of the **Avaya Configuration** window, expand **Avaya** and **Administration**.
3	In the **Avaya Applications Configuration** window, click **Backup & Restore**.
4	On the **Contact Center Manager Administration - Backup and Restore** utility, click the **Restore** tab.
5	Click **Browse** and select the backup file. Backup files are stored in a .package format.
6	Click **Start Restore**.

7 Update the URL that refers to the Contact Center Manager Administration server on all client PCs.

8 If your registry settings are unchanged, skip to step step 18.

OR

If you restore to a new server, or if your registry settings are corrupted or overwritten, continue to step step 9 to manually reconfigure your Real-Time Reporting and Emergency Help configuration settings and to ensure these settings are the same as they were before the restore.

9 Click **Start, All Programs, Avaya, Contact Center, Manager Administration, Configuration**.

10 In the left pane of the Configuration window, click on the **Real-Time Reporting** folder.

11 In the right pane, click the **RTR Registry Settings** icon.

12 In the **RTR Registry Settings** dialog box, reenter all settings that you recorded for the Real-Time Reporting and Emergency Help configurations.

13 Click **OK**.

14 In the left pane of the Configuration window, click on the **Emergency Help** folder.

15 In the right pane, click on the **Emergency Help Registry Settings** icon.

16 In the **Emergency Help Properties** dialog box, reenter all settings that you noted when you backed up the Real-Time Reporting and Emergency Help configurations.

17 Click **OK**.

18 Restore the Security Framework if it is installed co-resident with Contact Center Manager Administration.

--End--

Restoring Security Framework data

Restore Security Framework data in the following situations:

- if you recover from a server hardware failure.
- if you lose data or need a previous version of the data.
- if you migrate data to a new server.

Prerequisites

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

Procedure steps

Step	Action
1	On the Security Framework server, click **Start, All Programs, Avaya, Contact Center, Security Framework, Backup and Restore**.
2	In the **Security Framework - Backup and Restore** utility, select the **Restore** tab.
3	Click **Restore Files**.
4	Use the **Backup and Restore Wizard**, click **Next**. **OR** On the **Windows Server Backup** utility, click the **Restore and Manage Media** tab.
5	Click the **Restore and Manage Media** tab.
6	In the left pane, select the most recent backup file (or the file containing the data to restore).
7	Expand the file.
8	Select the check box for each file to restore. To select all the files, select the check box beside the parent file name.
9	Ensure you select the option to always replace the files on the computer.
10	Ensure that Original location appears in the **Restore files to** list.
11	Click **Start Restore**.
12	Choose **Start**, **All Programs**, **Avaya**, **Contact Center**, **Security Framework**, **Security Settings**.
13	Select **Restart Security Framework**.
14	Click **Close**.

--End--

Switching to the standby server in Agent Desktop Display

Switch to the standby server in Agent Desktop Display if the primary server fails, if you have a replicating server installed, and if you configured your Agent Desktop Display with IP addresses for standby servers.

The IP addresses of the standby server are configured when you installed and configured Agent Desktop Display on the client.

Procedure steps

Step	Action
1	On each agent workstation, click **Start, All Programs, Agent Desktop Displays, Server IP Addresses Configuration**.
2	In the **Server Configuration** dialog box, select the standby server.

--End--

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 (page 188)
- Choosing AD-LDS service accounts (page 190)
- Stopping replication on replicating servers (page 191)
- Starting replication on replicating servers (page 191)

Setting up AD-LDS replication

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.

Prerequisites

- 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.

Procedure steps

Step	Action
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.

--End--

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

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.

Prerequisites

- 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.

Procedure steps

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

--End--

Procedure job aid

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

Stop AD-LDS replication on all replicating servers.

Procedure steps

Step	Action
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 +DISABLE_OUTBOUND_REPL**.
6	Press **Enter**.
7	Close all windows.

--End--

Starting replication on replicating servers

Start AD-LDS replication on all replicating servers.

Procedure steps

Step	Action
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 -DISABLE_OUTBOUND_REPL**.
6	Press **Enter**.
7	Close all windows.

--End--

Contact Center Manager Administration failure recovery

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

For more information about restoring Contact Center Manager Administration data after a failure, see Restoring the Contact Center Manager Administration database (page 195).

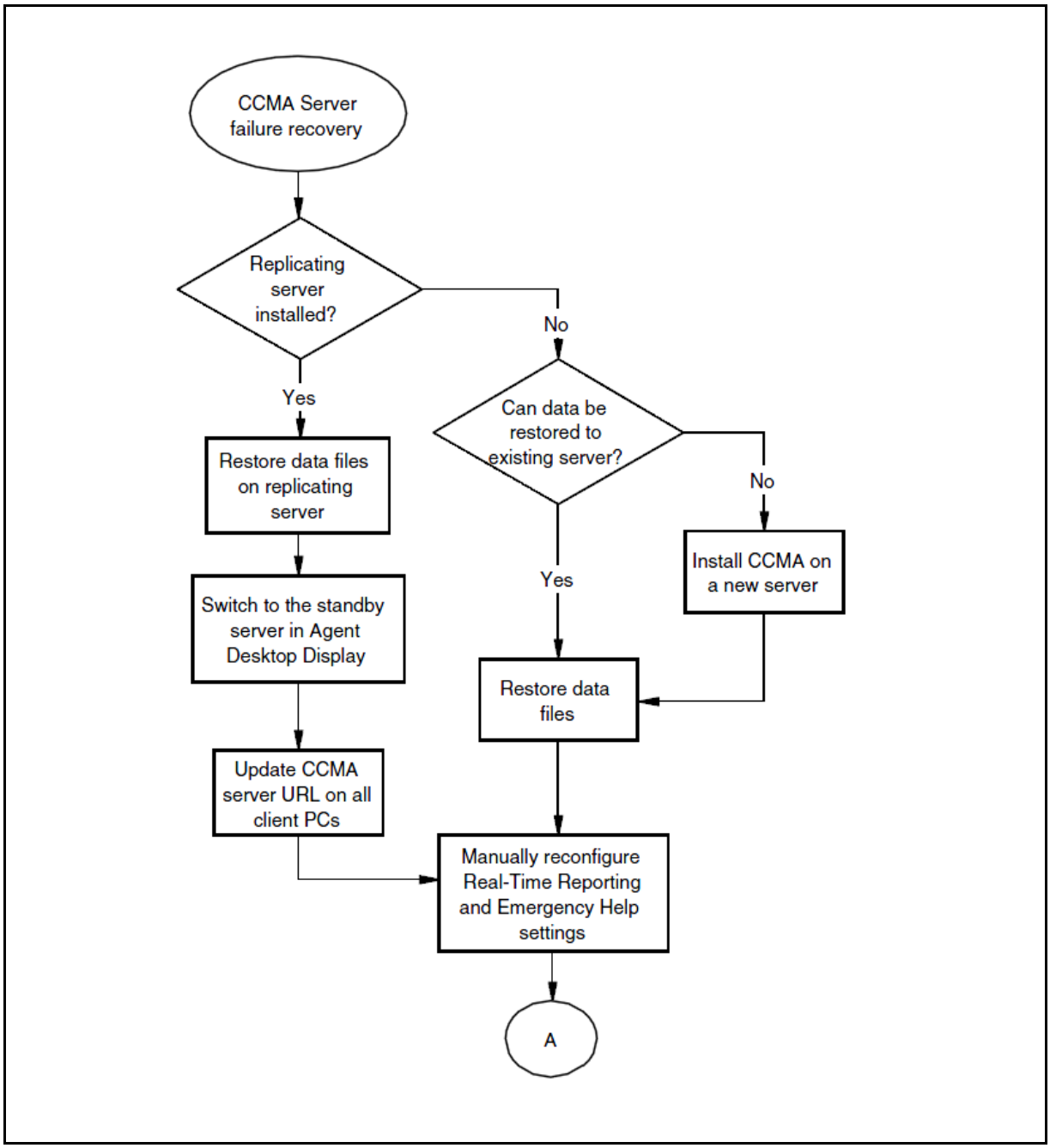
Prerequisites for Contact Center Manager Administration server failure recovery

- The Windows Server 2008 - Windows Server Backup utility must be installed on the Contact Center Manager Administration server.
- 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.
- Retain the permission properties of the AD-LDS data directory and AD-LDS files if you restore these files (for example, you must retain permissions such as NETWORK SERVICE). If you do not maintain permission properties, the SymposiumWC service does not start.

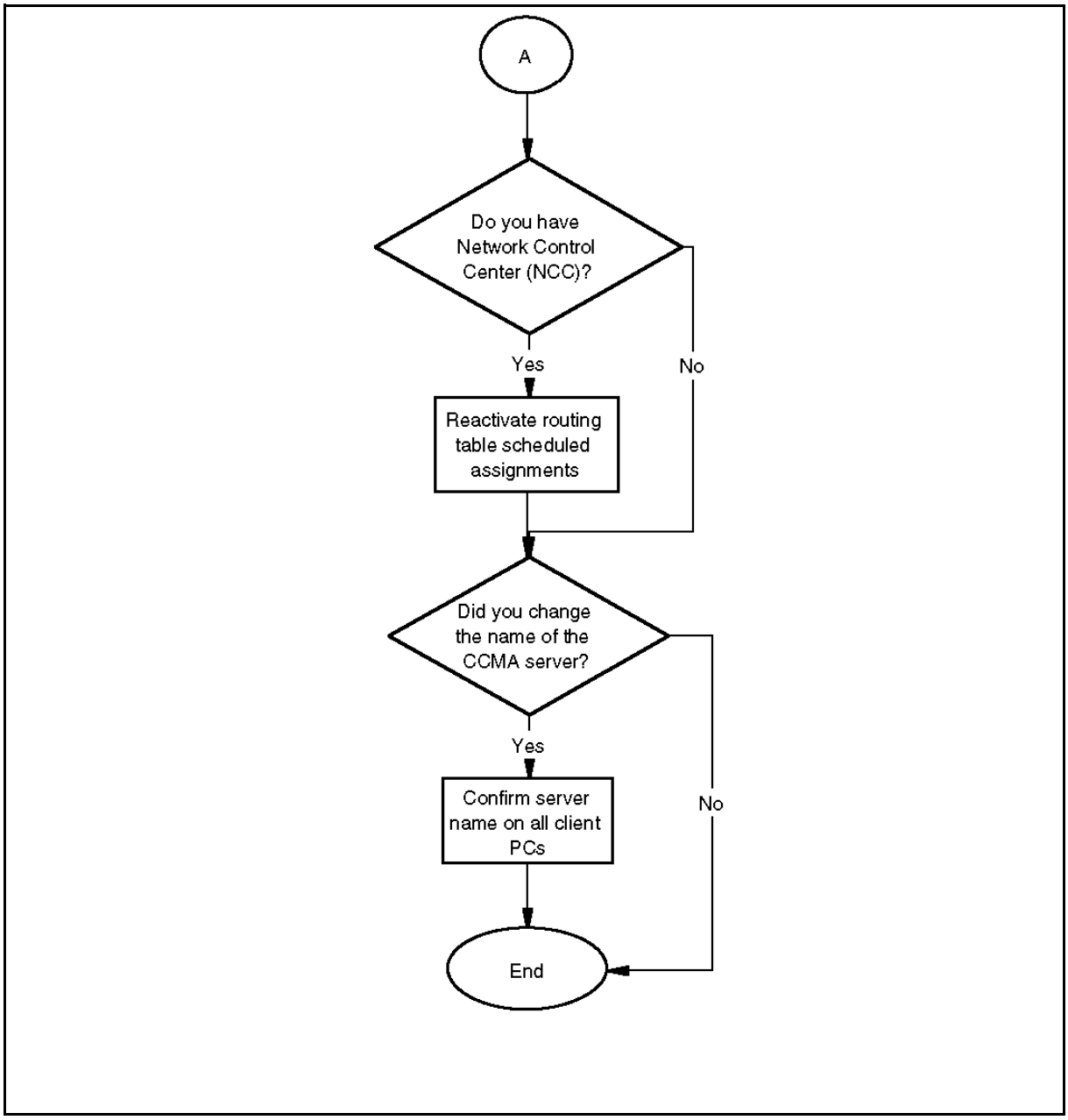
Contact Center Manager Administration server failure recovery procedures

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.

Contact Center Manager Administration server failure recovery procedures



Contact Center Manager Administration server failure recovery procedures (continued)



Restoring the Contact Center Manager Administration database

Restore the Contact Center Manager Administration database to recover after a failure.

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 after a failure, you must restore these files using the Backup & Restore utility.

Prerequisites

- Know the network location (in Universal Naming Convention (UNC) format) of the drive for the backed up database.

Attention: Ensure that the target server has the same patch level as the source server.

Procedure steps

Step	Action
1	On the working Contact Center Manager Administration server, choose **Start**, **All Programs**, **Avaya, Contact Center**, **Manager Administration**, **Configuration**.
2	In the left pane of the **Avaya Configuration** window, expand **Avaya, Applications, Backup & Restore**.
3	In the right pane, click **Backup & Restore**.
4	In the **Contact Center Manager Administration - Backup And Restore** dialog box, click the **Restore** tab.
5	To select a backup file to restore from, click **Browse**.
6	In the **Select a backup file** dialog box, select the required .package file.
7	Click **Open**.
8	To restore the backup file data into CCMA, click **Restore Files**. *A **The restore completed successfully** message box appears.*
9	Click **OK**.

--End--

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

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 (page 197)
- Language family compatibility (page 198)

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, 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

Latin-1 includes all Western European languages that use the Latin-1 character set. French, German, 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 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.

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

- Obtaining a server certificate from the Security Framework (page 202)
- Obtaining a server certificate from a third-party authority (page 203)
- Installing a server certificate (page 204)
- Configuring the Contact Center Manager Administration security details (page 204)
- Disabling the Security Framework (page 206)
- Saving the root certificate authority to a file (page 206)
- Importing the root certificate authority to Internet Explorer (page 207)
- Configuring security prompts in Internet Explorer (page 207)
- Viewing the security server settings (page 208)

Obtaining a server certificate from the Security Framework

Obtain a server certificate from the Security Framework. The Security Framework installs its own certification authority to use to sign a certificate request to secure the Contact Center Manager Administration Web site using an X.509 interface. You need this certificate to run Contact Center Manager Administration over a secure channel, such as HTTPS.

Once you create the certificate request using the Web Server Certificate Wizard this certificate must be signed before it is installed. This certificate can be signed using SFW Certificate Authority by using the Agent Certificate Configuration utility provided with the CCMA server.

If the request is successful, you receive a server certificate that you must install using the Web Server Certificate Wizard. For more information, see Installing a server certificate (page 204).

Prerequisites

- Install Internet Information Services Manager on the Contact Center Manager Administration server.
- Install and configure the Security Framework.

Procedure steps

Step	Action
1	Click **Start**, **Administrative Tools**, **Internet Information Services (IIS) Manager**.
2	Double-click the local computer, and then double-click the **Web Sites** folder.
3	Right-click the Web site or file for which you want to request a certificate, and then click **Properties**.
4	Click on the **Directory Security** tab if you selected a Web site **OR** Click on the **File Security** tab if you selected a file.
5	In the **Secure communications** group, click **Server Certificate**.
6	In the Web Server Certificate Wizard, follow the prompts to renew or create a new certificate.
7	Click **Prepare the request now, but send it later**.
8	Complete the remaining steps in the Web Server Certificate Wizard, and then click **Finish**.
9	On the CCMA server where you generated the certificate request, click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Manager Administration** to run the Client Certificate Management utility.
10	Type the fully qualified domain name of the SFW server to sign the certificate request.
11	Type a valid User ID and Password for this server.

12 Select the certificate request file created by the Web Server Certificate Wizard.

13 Click **Process Request**.

Two files are created in the folder from where you select the certificate request file. The ClientCertificate.cer file is the certificate file that you install on your Web server. The RootCACertificate.cer file is the root CA certificate file that you add to your Trusted Root Certification Authorities on each of your clients.

--End--

Obtaining a server certificate from a third-party authority

Obtain a server certificate from a third-party certification authority to secure the Contact Center Manager Administration Web site using an X.509 certificate. You need this certificate to run Contact Center Manager Administration over a secure channel, such as HTTPS.

After you request a server certificate from a third-party certification authority, the request is processed. If the request is successful, you receive a server certificate that you must install using the Web Server Certificate Wizard. For more information, see Installing a server certificate (page 204).

Prerequisites

- Install IIS Manager on the Contact Center Manager Administration server.

Procedure steps

Step	Action
1	Click **Start**, **Administrative Tools**, **Internet Information Services (IIS) Manager**.
2	Double-click the local computer, and then double-click the **Web Sites** folder.
3	Right-click the Web site or file for which you want to request a certificate, and then click **Properties**.
4	Click on the **Directory Security** tab if you selected a Web site **OR** Click on the **File Security** tab if you selected a file.
5	In the **Secure communications** group, click **Server Certificate**.
6	In the Web Server Certificate Wizard, follow the prompts to renew or create a new certificate.
7	Click **Prepare the request now, but send it later**.
8	Complete the remaining steps in the Web Server Certificate Wizard, and then click **Finish**.

--End--

Installing a server certificate

Install a server certificate after you request and receive a server certificate from a third-party certification authority. You need this certificate to run Contact Center Manager Administration over a secure channel, such as HTTPS.

Prerequisites

- Ensure that you received a server certificate. For more information, see Obtaining a server certificate from a third-party authority (page 203).

Procedure steps

Step	Action
1	Click **Start**, **Administrative Tools**, **Internet Information Services (IIS) Manager**.
2	Double-click the local computer, and then double-click the **Web Sites** folder.
3	Right-click the Web site or file for which you requested and received a certificate, and then click **Properties**.
4	Click on the **Directory Security** tab if you selected a Web site. **OR** Click on the **File Security** tab if you selected a file.
5	In the **Secure communications** group, click **Server Certificate**.
6	In the Web Server Certificate Wizard, click **Process Pending Request**.
7	Perform the remaining steps in the Web Server Certificate Wizard, and then click **Finish**.

--End--

Configuring the Contact Center Manager Administration security details

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

Prerequisites

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

Procedure steps

Step	Action
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 Protcol**.

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.

--End--

Variable definitions

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

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 steps

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

--End--

Saving the root certificate authority to a file

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.

Prerequisites

- Ensure that you have a server certificate. For more information, see Obtaining a server certificate from a third-party authority (page 203).

Procedure steps

Step	Action
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.

--End--

Importing the root certificate authority to Internet Explorer

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.

Prerequisites

- 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 (page 206).

Procedure steps

Step	Action
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.

--End--

Configuring security prompts in Internet Explorer

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

Procedure steps

Step	Action
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.

--End--

Viewing the security server settings

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.

Prerequisites

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

Procedure steps

Step	Action
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**.

--End--

Security Commissioning

- User identity provisioning (page 211)
- Role creation and management (page 215)
- Element and permission mapping (page 217)
- Role mapping (page 221)
- Policy creation and management (page 223)
- External identity repository configuration (page 227)
- Element Management (page 233)
- Security log management (page 237)
- Account and password management (page 239)
- Session management (page 243)

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 (page 211)
- Adding an external account (optional) (page 212)

Adding a local user identity and password

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

Procedure steps

Step	Action
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**.

--End--

Variable definitions

Variable	Value
Local	Specifies a user who is authenticated locally in Unified Communications Management (UCM).
Full Name	The user's full name, 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)

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.

Prerequisites

- Provision an external server. For more information, see External identity repository configuration (page 227).

Procedure steps

Step	Action
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 **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**.

--End--

Variable definitions

Variable	Value
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 user's full name, 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 _ .

Role creation and management

Create and manage roles to control user access to elements.

Navigation

- Creating a custom role (page 215)
- Deleting a custom role (optional) (page 216)

Creating a custom role

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 steps

Step	Action
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**.

--End--

Variable definitions

Variable	Value
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)

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

Prerequisites

- You must create a custom role.

Procedure steps

Step	Action
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**.

--End--

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 (page 217)
- Mapping elements and permissions by copying from another role (page 218)
- Removing elements from a role (optional) (page 219)

Mapping elements and permissions to a role

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

Procedure steps

Step	Action
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 Elements To Map to Role** page, in the **Element Name** list, select the element you want to map to the role.
7	Click **Next**.
8	On the **Permission Mapping** page, in the list next to each management function, select a permission setting (Deny, View, or Modify).
9	Optionally, select the **Allow use of Element Manager** check box.
10	Click **Save**.

--End--

Variable definitions

Variable	Value
Allow use of Element Manager	Select this check box to allow users with this role to use Element Manager.
Deny	Prevents users with the role from using the specified management function.
View	Allows users with the role to view but not modify the specified management function.
Modify	Allows users with the role to view and modify the specified management function.

Mapping elements and permissions by copying from another role

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

Procedure steps

Step	Action
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**.

--End--

Removing elements from a role (optional)

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

Procedure steps

Step	Action
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**.

--End--

Role mapping

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

Navigation

- Assigning roles to a user (page 221)
- Assigning users to a role (page 222)

Assigning roles to a user

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 (page 218).

Procedure steps

Step	Action
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**.

--End--

Assigning users to a role

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

Procedure steps

Step	Action
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 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**.

--End--

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 (page 223)

Creating a security policy for passwords

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 steps

Step	Action
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**.

--End--

Variable definitions

Variable	Value
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 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.

Variable	Value
Minimum age	The minimum allowable days for a password age. A minimum age prevents password recycling that could otherwise defeat the history policy. Valid values are 0 to 7 days. The user's new password 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 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.

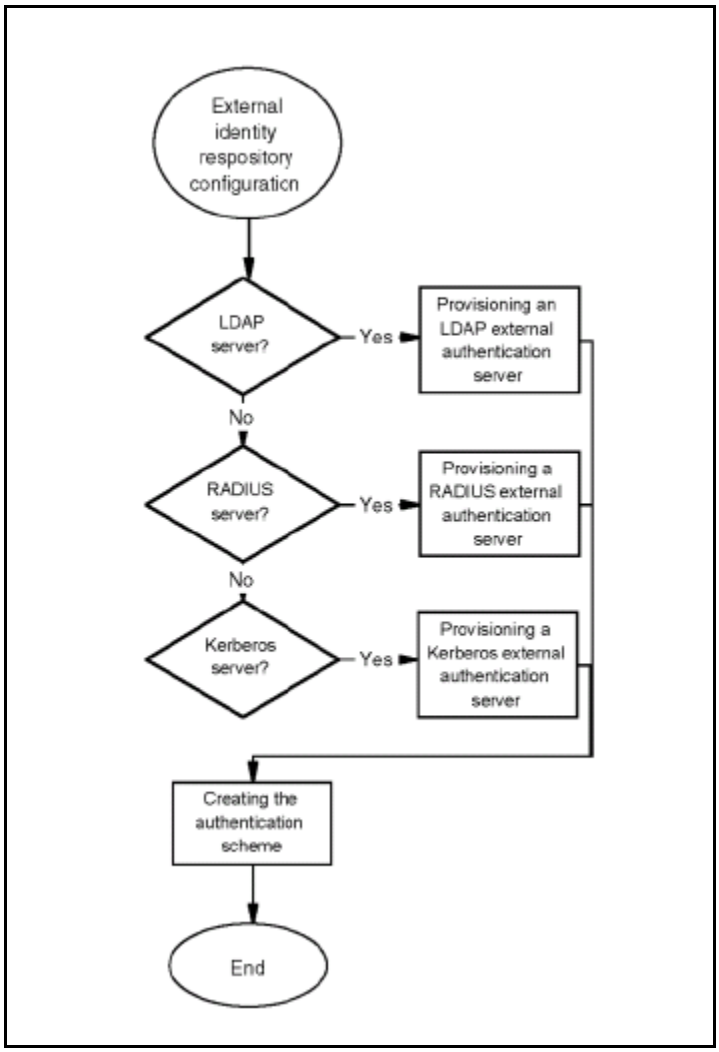
External identity repository configuration

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

External identity repository configuration procedures

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 (page 227).

External identity repository configuration procedures



External identity repository configuration navigation

- Provisioning an LDAP authentication server (page 228)
- Provisioning a RADIUS authentication server (page 229)

- Provisioning a Kerberos authentication server (page 230)
- Creating an authentication scheme (page 231)

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

Provisioning an LDAP authentication server

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

Procedure steps

Step	Action
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**.

Attention: 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.

--End--

Variable definitions

Variable	Value
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 authentication server

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

Procedure steps

Step	Action
1	Log on to Unified Communications Management as a security administrator.
2	In the navigation pane, click **User Service, 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**.

--End--

Variable definitions

Variable	Value
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 authentication server

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 SCE. In SCE, if the session values expire, you must re-authenticate through Contact Center Manager Administration, and then log on to SCE.

Procedure steps

Step	Action
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**.

--End--

Variable definitions

Variable	Value
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 an authentication scheme

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

Prerequisites

- Configure at least one external authentication server.

Procedure steps

Step	Action
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 Contact Center should use to authenticate users.

Attention: The number of options on the Authentication Scheme page depends on the number of external authentication servers in your system.

5 Click **Save**.

--End--

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) (page 233)
- Editing a secured element (optional) (page 234)
- Deleting a secured element (Optional) (page 234)

Adding a new Contact Center application (Optional)

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

Prerequisites

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

Procedure steps

Step	Action
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.

Attention: 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.

--End--

Variable definitions

Variable	Value
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 MAS>:8443

Editing a secured element (optional)

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

Prerequisites

- Add an element. For more information, see Adding a new Contact Center application (Optional) (page 233).

Procedure steps

Step	Action
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.

--End--

Deleting a secured element (Optional)

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

Prerequisites

- Add an application. For more information, see Adding a new Contact Center application (Optional) (page 233).

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

Procedure steps

Step	Action
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.

Attention: 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.

--End--

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 (page 237)
- Downloading and inspecting security logs (page 237)

Inspecting security logs

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

Procedure steps

Step	Action
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.

--End--

Downloading and inspecting security logs

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

Procedure steps

Step	Action
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 .txt 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 .txt file, and double-click the file to open the file and view the contents.

--End--

Account and password management

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

Navigation

- Changing your password (page 239)
- Resetting a user password (page 240)
- Disabling a user account (optional) (page 241)
- Reenabling a user account (optional) (page 241)
- Deleting a user account (optional) (page 242)

Changing your password

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.

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

Procedure steps

Step	Action
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**.

--End--

Variable definitions

Variable	Value
New password	The new password for the administrator account. Allowed characters in the password are: a-z A-Z 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

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.

Prerequisites

- 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.

Procedure steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
Password	The password used to log on to ECM. Allowed characters in the password are: a-z A-Z 0-9 { } | ( ) , / . = [ ] ^ ~ _ @ ! ‘ ; The password is a minimum of 8 characters long.

Disabling a user account (optional)

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 steps

Step	Action
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**.

--End--

Reenabling a user account (optional)

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 steps

Step	Action
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**.

--End--

Deleting a user account (optional)

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 steps

Step	Action
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**.

--End--

Session management

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

Navigation

- Viewing active sessions (page 243)
- Ending sessions manually (page 243)

Viewing active sessions

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

Procedure steps

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

--End--

Ending sessions manually

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

Procedure steps

Step	Action
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**.

--End--

Network Control Center Server

- Networking Service Monitor configuration (page 247)
- Network Control Center server administration (page 251)

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 (page 247)
- Closing the Networking Service Monitor (page 248)
- Refreshing the service status (page 248)
- Setting the default site information (client machine) (page 249)
- Adding a site (page 249)

Changing the site to monitor

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

Procedure steps

Step	Action
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.

--End--

Closing the Networking Service Monitor

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

Procedure steps

Step	Action
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.

--End--

Refreshing the service status

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 steps

Step	Action
1	Click **Refresh All** to refresh the status of all services.
2	Double-click a service in the list to refresh the status.

--End--

Setting the default site information (client machine)

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 steps

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

--End--

Adding a site

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

Prerequisites

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

Procedure steps

Step	Action
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**.

--End--

Network Control Center server administration

Configure the Network Control Center server to enable skillset routing in your Avaya Aura™ Contact Center.

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 (page 252)
- Adding access classes (page 253)
- Adding a site in Contact Center Manager Administration (page 254)
- Configuring network communication parameters (page 255)
- Synchronizing site information (page 257)
- Adding a network skillset (page 258)
- Configuring network skillset properties (page 259)
- Configuring Agent Order Preference (page 260)
- Configuring the routing tables (page 260)
- Configuring routing table assignments (page 261)
- Configuring the historical statistics collection (page 263)
- Configuring MCDN network CDNs (page 263)
- Configuring DNIS Network CDNs (page 265)

Adding a site to the NCC

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.

Prerequisites

- Log on to the Network Control Center server as Administrator.
- Know the CLAN IP address for each server to add.

Attention: Each server must have a unique CLAN IP address.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Manager Server**, **Network Configuration**.
2	In the **Nbconfig** dialog box, click the **Site Table** tab.
3	Click **Add**.
4	In the **Add Site** dialog box, in the **CLAN IP Address** box, type the CLAN IP address of the server.
5	Click **OK**. *The server is added to the list in the site table.*
6	Repeat step 3 to step 5 for each server in your network.
7	Click **Verify**. *This verifies the connection to the nodal servers.*
8	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.*
9	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.*
10	Click the **Address Table** tab. *The communication addresses of the new servers appear on the Address Table page.*

--End--

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

Adding access classes

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 steps

Step	Action
1	Log on to the Contact Center Manager Administration client.
2	On the launch pad, 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**.

--End--

Adding a site in Contact Center Manager Administration

A site is a location in the network with a telephony PABX and a server in Contact Center Manager Server. 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.

Prerequisites

- Make sure that each site is correctly configured before you add the next site.
- 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.

Procedure steps

Step	Action
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 dim.
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 all read-only 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 must add a CDN (Route Point) Landing Pad or a DNIS Landing Pad. Optionally, you can add both.

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.

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.

--End--

Configuring network communication parameters

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 steps

Step	Action
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 should 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.

--End--

Synchronizing site information

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 steps

Step	Action
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.

--End--

Adding a network skillset

Add a network skillset to the process to assign 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.

Procedure steps

Step	Action
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.

--End--

Configuring network skillset properties

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 steps

Step	Action
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.

--End--

Configuring Agent Order Preference

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 steps

Step	Action
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.

--End--

Configuring the routing tables

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.

Prerequisites

- Add network skillsets.

Procedure steps

Step	Action
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 to step 9 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.

--End--

Configuring routing table assignments

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.

Prerequisites

Attention: 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.

Procedure steps

Step	Action
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 to step 9 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.

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.

Attention: 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.

--End--

Configuring the historical statistics collection

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 steps

Step	Action
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 3 days, but you retain call-by-call statistics for 2 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.

--End--

Configuring MCDN network CDNs

Configure MCDN network CDNs 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.

Prerequisites

Attention: 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 – Service Creation Environment 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 CS1000 Integration* (NN44400-512).

Procedure steps

Step	Action
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.

--End--

Configuring DNIS Network CDNs

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.

Prerequisites

- 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 CS1000 Integration* (NN44400-512).

Procedure steps

Step	Action
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 CS1000 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.

--End--

Communication Control Toolkit Server

- Communication Control Toolkit fundamentals (page 269)
- Server settings configuration (page 275)
- Resource management (page 281)

Communication Control Toolkit fundamentals

The Communication Control Toolkit server 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 (page 269)
- Communication Control Toolkit Administration tool (CCT Console and Web Administration) (page 270)
- Contact Management Framework (page 270)
- Trace Control Utility (page 270)
- Resources (page 270)
- Programming interfaces (page 272)
- Communication Control Toolkit Reference Client (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

Avaya provides a separate application called ACDProxy Service. This application allows the agents to log on, log off, and go ready or 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 tool (CCT Console and Web Administration)

The CCT Console, or Avaya Communication Control Toolkit Console is a software component on the Communication Control Toolkit server that is used for server-side and bulk configuration tasks only.

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.

CCT Web Administration starts from the Contact Center Manager Administration (CCMA) server. In a knowledge worker environment without CCMA installed, the CCT Web Administration application is accessed on the CCT server by using a URL of the format http://<CCT IP address>:8081/WebAdmin.

Contact Management Framework

The Contact Management Framework (CMF) is a central repository for objects representing communications, including endpoints (terminals and addresses), transactions (contacts), and the relationships between them. The CMF includes the contact, resource, and agent managers. The CMF is also an abstraction or unification layer for various communications PABX interfaces. The Communication Control Toolkit API objects have a one-to-one mapping with the objects in the CMF.

The CMF is driven by one or more PABX interface service providers (for example, a connector for Avaya Communication Server 1000 communications or a SIP provider for SIP-enabled contact center). The PABX interface service provider updates the CMF objects to reflect the status of the PABX and to monitor the objects in the CMF for requests that objects pass to the PABX.The CMF is configured using the deployment type configuration in the CCT Snap-in.

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.

Resources

Configure the following resources in Communication Control Toolkit:

- Windows user—Users who are logged on to one or more communication terminals.
- Windows user group—A logical group of Windows users (for example, a sales group or a support group) that have a common property.
- Agent—Agents that are configured in the contact center database on Contact Center Manager Server with a designated role in the contact center such as a supervisor or an agent to received queued contacts.

- Agent group—A logical group of agents (for example, agents or supervisors) that have a common property.
- Terminal—A physical (including software applications) communications endpoint such as an e-mail client or an IVR line. Two terminal types indicate the types of physical communication endpoints:
  - Agent—An agent terminal can log on to an ACD queue and answer calls routed to that queue (if scripted). An Agent terminal can also make calls.
  - Knowledge Worker—A knowledge worker terminal cannot log on to an ACD queue or answer calls routed to a queue. A knowledge worker terminal can make and answer regular calls.
- Terminal group—A logical group of terminals (for example, local office, support office) that have a common property.
- Address—A logical communications endpoint such as an e-mail address or phone number. An address can be one of three types:
  - Basic—A basic address (SCR key) is an address that has an associated terminal (physical endpoint). The basic address is used by Communication Control Toolkit users to answer and make calls.
  - Route Point—A route point address (CDN) is an address to a terminal that is not associated with a line. The Route Point address is used by the Telephony Service Provider to accept incoming contacts or as a point to which contacts are routed.
  - Agent—A position ID (ACD key) for the Avaya Communication Server 1000 PABX.
- Address group—A logical group of address that have a common property.
- Workstation—A computer used by Communication Control Toolkit client operations on the same domain as the Communication Control Toolkit server.
- Network IVR—In a networked environment, the Network IVR driver uses information stored in the remote host address table to request call data for inbound calls overflowed from a remote Avaya Communication Server 1000. The first entry on the Network IVR port for local CCT Server has a fixed 127.0.0.1 IP address and this can not be changed. This first entry can not be deleted.
- Provider—A PABX interface service provider to connect telephony devices to the Communication Control Toolkit server. Two provider types are available:
  - Passive (for voice contacts)

Resource Assignments

Assignments use the following principles:

- When a terminal is assigned to an agent, CCT automatically assigns the terminal's associated addresses to the respective agent. When the agent logs in CCT checks changes to the agent's configuration. Any new addresses assigned to the terminal

are automatically assigned to the agent. Also, any un-assigned addresses, are automatically un-assigned from agents.

- Assignments are distributed using groups. If you assign one resource to a second resource that is a group, and the second resource to a third, then the first resource also assigns to the third. For example, if you assign two users to a user group, and then assign the user group to an address, the users are considered assigned to the address. Or, if you assign a user to a user group, the user inherits the user group terminals and addresses.
- Only terminals are assigned to workstations.
- When you assign a terminal to a user, you must assign an address.
- You do not assign route point addresses to terminals, route point addresses do not have associated terminals.
- Resource groups are collections of resources. For example, User groups are collections of users.

Possible resource-to-resource assignments

Resource	Assignment
User	Terminals, Addresses, Terminal Groups and Address Groups can be assigned to a User
Terminal	Addresses and Workstations can be assigned to Terminals
Address	No resources can be assigned to an Address
Workstation	No resources can be assigned to an Workstation

Programming interfaces

When you configure your CCT server, your CCT users log on with user accounts based on 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, 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 re-create 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.

Server settings configuration

This section outlines the procedures necessary to configure the Communication Control Toolkit server settings:

- Contact Center server License details
- Contact Center Deployment Type
- Avaya Communication Server 1000 provider details

Navigation

- Configuring the licensing for CCT (page 275)
- Configuring the deployment type for CCT (page 276)
- Configuring the Avaya Communication Server 1000 service provider (page 278)

Configuring the licensing for CCT

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.

Prerequisites

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

Procedure steps

Step	Action
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 the right pane License Configuration, 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.

Attention: The Secondary License Manager Server IP Address section is only available 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**.

--End--

Variable definitions

Variable	Value
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 only available 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 the deployment type for CCT

Configure the deployment type for the CCT server to manage the contact routing for your network configuration.

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

Prerequisites

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

Procedure steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
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.

Configuring the Avaya Communication Server 1000 service provider

Configure the Avaya Communication Server 1000 service provider details to enable connection to the PABX. A polling message is sent every ten seconds to monitor the connection the PABX. The polling interval detail is configured in the Communication Server 1000 service provider details. Ten seconds is the default polling time.

Prerequisites

- Understand the server provider details for the switch.

Procedure steps

Step	Action
1	Log on to Contact Center Manager Administration server.
2	Launch Communication Control Toolkit Web Administration client.
3	In the resource menu list, select **Providers**. *The details of the providers are displayed.*
4	Select **Passive** from the list of providers.

5 In the **Basic Provider Information** section, in the **Passive Name** box, type the Provider name.

Attention: The provider name must be “Passive”.

6 Select the **Enabled** tickbox, to enable the provider.

7 In the **IP Address** box, type the IP address of the provider.

8 In the **Port** box, type the port number.

9 In the **Provider Configuration** section, select the **Transport** type, **TCP.**

10 In the **Customer Number,** type the customer number.

11 In the **CS1000 Software Release**, select the correct version.

12 In the **Call Data Life Span (minutes)**, type the required value in minutes.

13 Select or clear the **Disable Copy of Data to Consult Call** check box.

14 In the **CS1000 Home location Code (HLOC)**, type the HLOC value.

15 In the **Network IVR Port**, type the port value.

16 In the **Initialization Timeout (seconds)** box, type the **Initialization timeout** setting in seconds.

17 In the **Command Timeout (seconds)** box, type the **Command** timeout setting in seconds.

18 Select **Save**.

--End--

Variable definitions

Variable	Value
Provider Name	Name of the Provider, Passive.
IP Address	In a Contact Center environment, the IP address of the CCMS.
Enabled	Select to enable the provider.
Port	In a Contact Center environment, the default port value is 3000.
Transport	Transport protocol, default is TCP.
Customer Number	The customer number for the switch. If multiple customers are configured, you must specify a specific one in this box.
CS1000 Software Release	The release number of Avaya Communication Server 1000 software.

Variable	Value
Call data	Call data is the information attached to calls routed from the switch. The Life Span default is 10 minutes. This value must be less than the time it takes to recycle the Communication Server 1000 Call IDs. Use the Disable copy of call data to consultative call check box to avoid copying call data during consultative calls, but you can still copy call data when calls are transferred or conferenced.
CS1000 Home Location Code (HLOC)	Avaya Communication Server 1000 Home Location Code (HLOC) of the switch is the address digits that specify a location node.
Network IVR Port	Port for the CCT network call attached data and for IVR call attached data.
Timeout in Seconds	Initialization—The length of time that the service provider waits to establish communication with the switch before generating an error. The default and minimum value is 32 seconds. If you use a large number of lines, you must increase this value accordingly. Command—The length of time that the service provider waits for a command response before generating an error. The default and minimum value is 5 seconds.

Resource management

Use the Communication Control Toolkit Administration Console and Web Administration to manage settings and resources in the database. The resources are used to map the voice and multimedia contacts to terminals and to route them to agents in the contact center. You can configure the resources manually or automatically using the Data Import/Export Tool.

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 from the Communication Control Toolkit domain (page 281)
- Importing Avaya Communication Server 1000 data (page 283)
- Importing workstations from the domain (page 286)
- Adding resources manually (page 287)
- Changing the properties of a resource (page 289)
- Assigning resources (page 289)
- De-assigning resources (page 291)
- Deleting resources (page 292)
- Importing bulk resources (page 292)
- Exporting Bulk Resources (page 293)
- Configuring Hotdesking (Agent Roaming) (page 295)

Importing Windows users from the Communication Control Toolkit domain

Import Windows users from the server to the Communication Control Toolkit administration tool using the Import Windows Users tool. After the resources are in the administration console, you can configure the resources in the CCT Web Administration client.

Prerequisites

- 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.

Procedure steps

Step	Action
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.
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**.

--End--

Variable definitions

Variable	Value
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

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 “Automatically import data after conversion”.

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 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.

Prerequisites

- 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.

Procedure steps

Step	Action
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.
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 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 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 Communication Server 1000 Provider.

30 Select **Input File**. This will open a file explorer to select the Communication Server 1000 data capture file you copied in step 23.

31 Select the Communication Server 1000 data capture file, click **Open**. A default path and file name is shown in the **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.

Attention: 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.

--End--

Importing workstations from the domain

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.

Prerequisites

- 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.

Procedure steps

Step	Action
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**.

--End--

Variable definitions

Search Type	Value
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.

Adding resources manually

Manually add resources such as Windows users, Windows users groups, Terminal, Terminal groups, Addresses, Address groups and Network IVR ports to organize your resources in the database. Use groups to arrange common single resources in your database into groups.

Note: To avoid errors, Avaya recommends that you use the CCT Console to add users, addresses, terminals, and workstations. See Importing Windows users from the Communication Control Toolkit domain (page 281), Importing Avaya Communication Server 1000 data (page 283), Importing workstations from the domain (page 286), and Importing bulk resources (page 292).

Prerequisites

- Know the name, properties, and mappings for the resource you are about to add to the database.

Procedure steps

Step	Action
1	Log on to the CCMA server.
2	Select **Configuration**.

3 Select the CCT Server.

4 Select **CCT Administration**.

5 Click **Launch CCT Console**.

6 In the **CCT Web Administration**, select resource type to add.

7 Right-click and choose **Add new resource**.

8 In the **required** boxes, type a unique information that you can easily recognize later.

9 If the new resource is a group, assign the individual resources to the group.

10 Add the assignments to the other resources according to the requirements of your contact center.

11 Click **OK**.

Attention: CCT Web Administration starts from the Contact Center Manager Administration (CCMA) server. In a knowledge worker environment without CCMA installed, the CCT Web Administration application is accessed on the CCT server by using a URL of the format http://<CCT IP address>:8081/WebAdmin.

--End--

Variable definitions

Variable	Definition
Address Group Name	A name for the address group.
IP Address	The IP address of the server you are currently using.
HLOC	The home location code of the Avaya Communication Server 1000 for the IVR system. This HLOC code is the same as the HLOC printed on the switch in overlay 21.
Port Address	The TCP IP port to which other nodes connect. Avaya recommends that you use port 5002 if the Communication Control Toolkit server is co-resident with Contact Center Manager Server.
Network IVR Description	A description of the Network IVR.
Terminal Group Name	A name for the terminal group.
User Group Name	A name for the user group.

Changing the properties of a resource

Change the properties of a resource, such as the assignments, name, or assigned group if the information for your contact center changes.

Procedure steps

Step	Action
1	Log on to the CCMA server.
2	Select **Configuration**.
3	Select the CCT Server.
4	Select **CCT Administration**.
5	Click **Launch CCT Console**.
6	Click the resource type to change.
7	From the list of resources in the right pane of the resource page, click the resource to change.
8	Make the changes to the assignment, name or assigned group using the buttoned tabs on the resource page.
9	Click **Save**.

Attention: CCT Web Administration starts from the Contact Center Manager Administration (CCMA) server. In a knowledge worker environment without CCMA installed, the CCT Web Administration application is accessed on the CCT server by using a URL of the format http://<CCT IP address>:8081/WebAdmin.

--End--

Assigning resources

Resources in CCT are users, terminals, addresses, and workstations.Create the contact center agents in CCMA before assigning resources in CCT. Creating the contact center agents in CCMA pushes the contact center windows user and agent information to the CCT database. This ensures all the data needed for assigning resources is in the CCT database, ready for configuration.

To enable CCT to work in a contact center follow the basic configuration:

- assign a terminal to one or two addresses
- assign a terminal to a workstation
- assign a terminal to a user.

Make configuration changes quickly in your contact center by organizing users, terminals and addresses into groups. This allows you to map your resource groups to functional roles in your contact center.

Use the Communication Control Toolkit Web Administration client to assign resources.

Procedure steps

Step	Action
1	Log on to the CCMA server.
2	Select **Configuration**.
3	Select the CCT Server.
4	Select **CCT Administration**.
5	Click **Launch CCT Console**.
6	Click the resource type.
7	Click the single resource to configure.
8	Select one of the Resource Assignments to assign to this resource.
9	Select the appropriate resources from those in the **Available Resources** column. Click each resource to select more than one resource or resource group. Select the resource again to deselect it.
10	Click **the Right Arrow** to move the selected resource and resource groups to the **Assigned Resources** column.
11	Click **Save**.

Attention: CCT Web Administration starts from the Contact Center Manager Administration (CCMA) server. In a knowledge worker environment without CCMA installed, the CCT Web Administration application is accessed on the CCT server by using a URL of the format http://<CCT IP address>:8081/WebAdmin.

--End--

Example of assigning resources

In a hotdesking configuration, CCT the resources are configured into groups.

Create a terminal group called hotdesking_terminals and assign all terminals to this group.

Assigning Terminals to a Terminal Group

Step	Action
1	Log on to the CCMA server.
2	Select **Configuration**.
3	Select the CCT Server.
4	Select **CCT Administration**.

5 Click **Launch CCT Console**.

6 Select **Groups**.

7 Select **Terminal Groups**.

8 Select the hotdesking_terminals terminal group.

9 Select the all terminals in the **Available Resources** column.

Click each resource to select more than one resource.

10 Click **the Right Arrow** to move the selected terminals to the **Assigned Resources** column.

11 Click **Save**.

--End--

De-assigning resources

De-assign resources in your Communication Control Toolkit **Web Administration** to remove the association between the resources to groups or other types of resources to delete resources efficiently.

Procedure steps

Step	Action
1	Log on to the CCMA server.
2	Select **Configuration**.
3	Select the CCT Server.
4	Select **CCT Administration**.
5	Click **Launch CCT Console**.
6	In the left resource menu, click the name of the resource to remove assignments.
7	Click the single resource name.
8	Select the appropriate resource assignments to update. Right click each resource to select more than one resource or resource group. Select the resource again to deselect it.
9	Click **the Left Arrow** to move the selected resource to the **Available Resources** column.
10	Click **Save**.

Attention: CCT Web Administration starts from the Contact Center Manager Administration (CCMA) server. In a knowledge worker environment without CCMA installed, the CCT Web Administration application is accessed on the CCT server by using a URL of the format http://<CCT IP address>:8081/WebAdmin.

--End--

Deleting resources

Delete resources from your Communication Control Toolkit database that you no longer require to save space. You can remove groups or individual resources.

Procedure steps

Step	Action
1	Log on to the CCMA server.
2	Select **Configuration**.
3	Select the CCT Server.
4	Select **CCT Administration**.
5	Click **Launch CCT Console**.
6	In the left resource menu, click the name of the resource to delete.
7	Select the individual resource to delete.
8	Right-click, and click **Delete**.
9	In the confirmation message dialog box, click **Yes**.

Attention: CCT Web Administration starts from the Contact Center Manager Administration (CCMA) server. In a knowledge worker environment without CCMA installed, the CCT Web Administration application is accessed on the CCT server by using a URL of the format http://<CCT IP address>:8081/WebAdmin.

--End--

Variable definitions

Variable	Definition
Resource type	The type of resource (Windows user, Terminal, Address, or Workstation to remove.

Importing bulk resources

Import bulk resources into the Communication Control Toolkit database using the Data Import/Export Tool of CCT Snap-in.

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.

Prerequisites

- Ensure that you have an XML file that matches the required file format to import the resources into the Communication Control Toolkit database.

Procedure steps

Step	Action
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 Setup select **Standard XML** or **Flattened XML** in the Format drop down box.
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.

--End--

Exporting Bulk Resources

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 steps

Step	Action
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 is exported to the file and the **Status** and **Total Records Exported** are shown in the status pane.

--End--

Variable definitions

Variable	Value
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 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.

Configuring Hotdesking (Agent Roaming)

In a contact center an agent may not have a fixed desk and phone. An agent might pick a desk that is not being used and log into the phone and workstation. An agent must be able to log onto any phone and workstation in this environment. This is called hotdesking or agent roaming, where an agent is not tied to one desk.

In a hotdesking environment using any configured workstation, agents can control the terminal and addresses associated with that workstation.

To enable hotdesking in CCT, a Windows user is assigned to multiple terminals; each terminal is assigned to it's respective workstation. The user's terminal is determined by the workstation that the user logs on to, as shown in the following example.

- Terminal_1 maps to workstation_1.
- Terminal_2 maps to workstation_2.

  For example, assume that User _1 is assigned to Terminal_1 and Terminal_2 and the respective addresses. If User_1 logs on to workstation_2, then the user also logs on to Terminal_2.

Prerequisites

- Create agents on the CCMA server and associate them with domain users.
- Assign each terminal to a workstation.
- Add terminals to a terminal group.
- Ensure that all terminals have the correct address assigned to them.
- If you require additional terminals (and therefore addresses) in the hotdesking group, add the new terminals to the terminal group and the new addresses to the address group. Follow this process to ensure that the correct resources are available to all roaming CCT agents at all times.

Procedure steps

Step	Action
1	Place all select terminals for hotdesking into a terminal group.
2	Ensure that all terminals have the correct address assigned to them.
3	Place all the addresses associated with the terminals into an address group.
4	Place all select users for hotdesking into a user group.
5	Assign the terminal group from step 1 to the user group from step 4 with the automatic mapping of addresses check box cleared.
6	Assign the address group from step 3 to the user group from step 4.
7	Assign each terminal to a workstation.

Attention: A terminal can only be assigned to one workstation.

--End--

Contact Center Multimedia

- Contact Center Multimedia fundamentals (page 299)
- General configuration (page 311)
- Outbound configuration (page 319)
- E-mail configuration (page 321)
- Voice Mail configuration (page 365)
- Fax configuration (page 369)
- Scanned document configuration (page 375)
- SMS configuration (page 381)
- Web communications configuration (page 387)
- Web communications customer interface configuration (page 399)
- Instant message configuration (page 415)
- Predictive Outbound administration (page 421)
- Agent Desktop configuration (page 427)
- Data collection and management (page 443)

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 6.0/6.1 include the following:

- voice contacts
- e-mail messages
- 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.

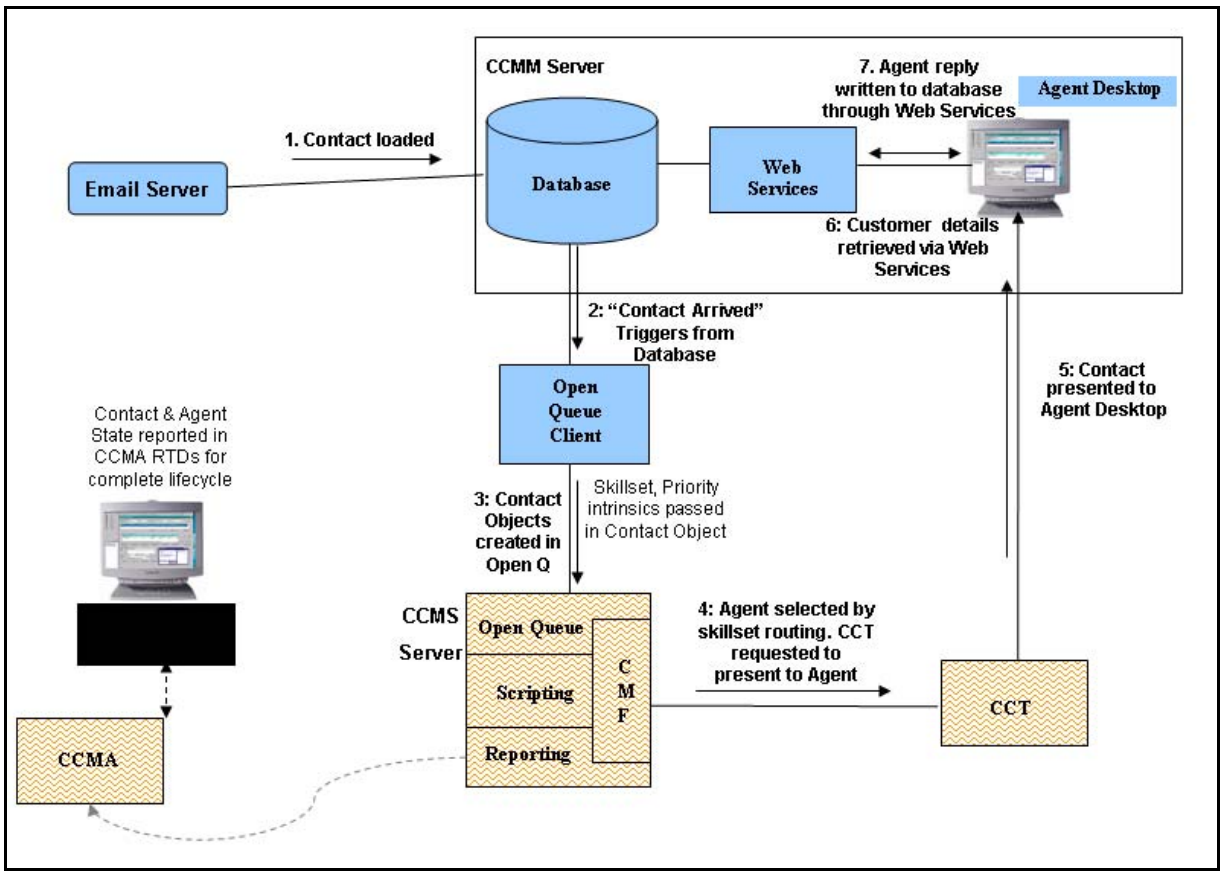
Navigation

- E-mail contact type (page 300)
- SMS text messages, faxes, scanned documents and voice mail attachments (page 305)
- Outbound contact type (page 307)
- Web communications (page 309)
- Instant Messaging (page 310)
- Office hours (page 310)

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.

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 (page 301)
- Recipient mailboxes (page 302)
- Inbound e-mail settings (page 302)

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 (page 302)
- Character encoding for outgoing e-mail messages (page 302)

You can configure the e-mail message contact type for international languages, see Asian e-mail (page 303).

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 (page 303).

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.

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 that you configure in the 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 customer's e-mail message. 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 the characters from East Asian languages is dangerous because of phishing sites. A phishing site is an e-mail message with a link to www.aib.ie can point you to a site that has the i and a b in the domain but some other character that resembles an a.

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 Email 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.

- Email (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.
- Email Progress shows the number of contacts in a new or closed state on a defined date to determine the traffic levels for that date.
- Email Closed Contacts Queue Time shows the average time an 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.

Agent Desktop

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).

Contact Center Manager Administration

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

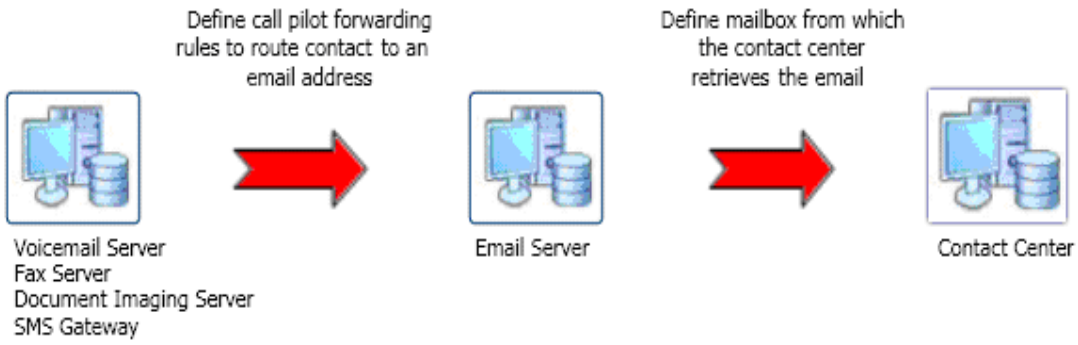
For each type of contact, you can configure the routing of the specified contact and assign a priority to the contact. See Mailbox configuration (page 306).

You can view traffic report summaries for each type of contact. See Traffic reports (page 306).

Use the Agent Desktop to open and reply to SMS, faxes, scanned documents, and voice mail contacts. See Agent Desktop (page 306).

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.

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.

Agent Desktop

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.

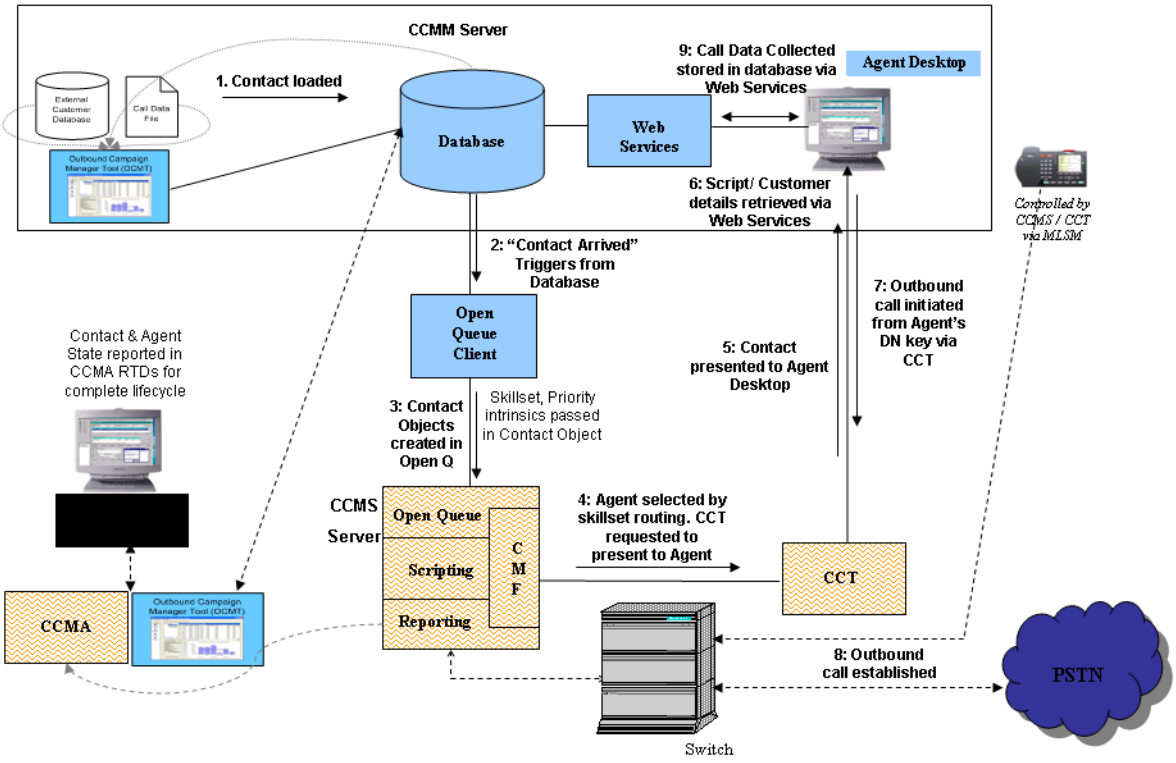
For more information about Agent Desktop, see the *Avaya Aura™ Agent Desktop User Guide* (NN44400-114).

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.

Outbound contact type routing



Contact Center Outbound consists of several components:

- Outbound Campaign Management Tool (page 308)
- Campaign Scheduler (page 308)
- Agent Desktop (page 308)
- Contact Center Manager Administration (page 309)

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.

Agent Desktop

Agents use Agent Desktop to process outbound contacts. When a campaign runs, outbound contacts are routed to Agent Desktop, and agents can perform the following activities:

- Accept or reject an outbound contact.
- Review and update customer information.
- Make the outbound voice call.
- Follow an agent script and record customers answers and comments.
- Select a disposition code to record the result of the call.

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

Contact Center Manager Administration

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

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 (page 311)
- Configuring the reporting credentials (page 312)
- Adding administrators (page 312)
- Removing administrators (page 313)
- Configuring office hours (page 314)
- Configuring holidays (page 315)
- Applying office hours (page 315)
- Viewing real-time traffic reports by contact (page 316)
- Configuring the displayed date for traffic reports (page 317)

Configuring the system license

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Configuring the reporting credentials

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Adding administrators

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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 the desired password and confirm it in the confirm password field.
8	Click **Save**.

--End--

Removing administrators

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

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Configuring office hours

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.

Prerequisites

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

Procedure steps

Step	Action
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 steps 6 and 7 for every day of the week.
9	Click **Save**.

--End--

Configuring holidays

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.

Prerequisites

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

Procedure steps

Step	Action
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**.

--End--

Applying office hours

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 (page 345).

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 (page 325).

Prerequisites

- Log on to the Contact Center Manager Administration application.
- Create a calendar template with office hours or holidays. See Configuring office hours (page 314) or Configuring holidays (page 315).

Procedure steps

Step	Action
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**.

--End--

Viewing real-time traffic reports by contact

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 (page 317).

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Configuring the displayed date for traffic reports

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

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 (page 319)

Configuring a route point for an Outbound skillset

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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 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**.

--End--

Variable definitions

Variable	Value
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.

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 mailbox 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 Email and View Reports in the left column of the Contact Center Multimedia application. You can choose the report date and the skillsets represented in all displayed real-time reports.

- 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 (page 323)
- Adding an e-mail server (page 324)
- Deleting an e-mail server (page 325)
- Configuring skillsets for e-mail (page 325)
- Creating or changing a recipient mailbox (page 326)

E-mail routing configuration

- Updating the system default rule (page 331)
- Updating the system delivery failure rule (page 333)
- Creating or changing a keyword group (page 335)
- Deleting a keyword from a keyword group (page 337)
- Deleting a keyword group (page 338)
- Creating or changing prepared responses (page 338)
- Removing attachments from prepared responses (page 342)
- Promoting suggested responses (page 342)
- Creating or changing a sender group (page 343)
- Deleting a sender group (page 344)
- Deleting a sender from a sender group (page 345)
- Creating or changing rules (page 345)
- Enabling a rule (page 348)
- Disabling a rule (page 349)
- Deleting a rule (page 349)
- Creating or changing rule groups (page 350)

Outgoing e-mail configuration

- Configuring the e-mail settings (page 351)
- Changing the character encoding for outgoing e-mail (page 354)
- Changing the character encoding of e-mail replies (page 355)
- Selecting the outgoing e-mail address (page 356)
- Barring e-mail addresses (page 356)

- Deleting a barred e-mail address (page 357)

Other e-mail configuration

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

Configuring the e-mail server names

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
1	In the Contact Center Manager Administration application, click **Multimedia**.
2	In the left column, select **General Administration**.
3	Click **Server Settings**.
4	In the **Server Settings** box, select **Inbound POP3 Server**.
5	In the **Primary Hostname** box, type the name of the server that receives or sends e-mail messages.
6	In the **Port Number** box, type the port number for the e-mail server.
7	If you have a backup e-mail server, in the **Secondary Hostname** box, provide a host name for the backup server.
8	Click **Save**.
9	In the **Server Settings** box, select **Outbound SMTP Server**.

10 In the **Primary Hostname** box, type the name of the server that receives or sends e-mail messages.

11 In the **Port Number** box, type the port number for the e-mail server.

12 If you have a backup e-mail server, in the **Secondary Hostname** box, provide a host name for the backup server.

13 In the **Advanced SMTP Authentication** box, select the SMTP authentication, if required, for your outbound e-mail server.

14 Click **Save**.

--End--

Variable definitions

Variable	Value
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

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step **Action**

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**.

--End--

Deleting an e-mail server

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

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Configuring skillsets for e-mail

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.
- If desired, configure an office hour template. See Configuring office hours (page 314) and Configuring holidays (page 315).

Procedure steps

Step	Action
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**.

--End--

Creating or changing a recipient mailbox

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.

Prerequisites

- 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.

Procedure steps

Step	Action
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	In the list box, 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. **Attention:** 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**.

--End--

Variable definitions

Variable	Value
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 Email 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. **Attention:** 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.
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

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.

Prerequisites

- 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 (page 326).
- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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 list box, 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.

Attention: When you change a password of the mail store recipient address on the email 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**.

--End--

Variable definitions

Variable	Value
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.
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 Email 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. **Attention:** 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

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.

Prerequisites

- 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.

Procedure steps

Step	Action
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.
5	Click **Delete**. A warning dialog box appears.
6	Click **Yes** to confirm to delete the recipient.

--End--

Updating the system default rule

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.

Prerequisites

- 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 (page 325).
- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
1	In the Contact Center Manager Administration application, click **Multimedia**.
2	In the left column, click **E-mail**.
3	Under **System Default Rule**, from the **Skillset** list, select a skillset name.
4	To change the automatic response settings, under **Auto Responses**, select another automatic response from the list.
5	To change the priority, under **Priority**, select a different priority for the contact.
6	Click **Save**.

--End--

Variable definitions

Variable	Value
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, “We received your e-mail and 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

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.

Prerequisites

- 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 (page 325).
- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
1	In the Contact Center Manager Administration application, click **Multimedia**.
2	In the left column, click **E-mail**.
3	Under **System Delivery Failure** Rule, from the **Skillset** list, select a skillset name.
4	To change the keyword group, under **Keyword Group**, select an existing keyword group from the list.
5	To change the priority, under **Priority**, select a different priority for the contact.
6	Select the **Will close contact** check box to have the rule to close the contact.
7	Click **Save**.

--End--

Variable definitions

Variable	Value
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

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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 **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 steps 6 through 9 to add more keywords to the list.
11	Click **Save**.

--End--

Variable definitions

Variable	Value
Name	Name of the keyword group. The name must be unique and less than 64 characters.
Keyword	A word, or string of characters, used to search the 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

Remove a keyword from a keyword group. The remaining keywords and phrases in the keyword group remain active for rules.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Deleting a keyword group

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Creating or changing prepared responses

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.

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

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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: automatic response or suggestion.
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: Beside the **Attachment** box, click **Add** to add attachments to the response.
10	Click **Save**.

--End--

Variable definitions

Variable	Value
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 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.

Procedure job aid

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

Prepared response toolbar



Style: Configured format for email.
Font: Character style to overwrite style.
Size: Character size to overwrite style.
Bold: Boldface text.
Italics: Italicize text.
Underline: Underline text.

Left align: Align all text on left.
Center: Center all text.
Right align: Align all text on the right.
Justify: Justify text on left and right.

Number: Number paragraphs.
Bullet: Place a bullet character in each paragraph.
Indent: Indent paragraph one tab.
Outdent: Outdent paragraph one tab.

Undo: Undo last change.
Redo: Redo last change.

Paint: Change color of text.
Highlight: Highlight selected text with color.
Line: Draw a line.

Link: Link to URL.
Graphic: Insert graphic into e-mail message.
Table: Insert table into e-mail message.

Deleting prepared responses

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

Procedure steps

Step	Action
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**.

--End--

Removing attachments from prepared responses

Remove attachments from a prepared response. The attachment file is stored on the Contact Center Multimedia server for later use.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Promoting suggested responses

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 the 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

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Creating or changing a sender group

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 steps

Step	Action
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 steps 5 through 8 to add sender addresses to this sender group.

10 Click **Save**.

--End--

Variable definitions

Variable	Value
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

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

Prerequisites

- You must have a sender group. See Creating or changing a sender group (page 343).

Procedure steps

Step	Action
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 **Remove**.

--End--

Deleting a sender from a sender group

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 steps

Step	Action
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**.

--End--

Creating or changing rules

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.

Prerequisites

- If you plan to use office hours for routing e-mail messages, configure your office hours. See Configuring office hours (page 314).
- Configure at least one e-mail skillset. See Configuring skillsets for e-mail (page 325).
- Create keyword groups, if required. See Creating or changing a keyword group (page 335).
- Configure prepared responses (automatic responses or suggestions), if required for the rule. See Creating or changing prepared responses (page 338).

Procedure steps

Step	Action
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**, click the plus sign (+) button. **OR** Select an existing rule.
5	In the **Input Criteria** area, under **Current Search Criteria**, choose the criterion to add to the rule.
6	Click **Go**.
7	Configure the keyword match or sender group to use.
8	Repeat steps 5 to 7 to select a maximum of five criteria for the rule.
9	Under **Current Search Criteria**, choose the weighting for each criterion. The total weighting must add up to 100 percent.
10	Under **Current Search Criteria Summary**, click the blue text to view the details of each criterion you configure.
11	Click **Next**.
12	To select an automatic response for the rule, under **Available Auto Response**, select the configured automatic response, and then click **>**.
13	To select automatic suggestions for the rule, under **Available Auto Suggest**, 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.
14	Click **Next**.
15	In the **General Settings** area, in the **Name** box, type a name for the rule.
16	In the **Skillset** box, select the skillset to apply for the rule.
17	In the **Priority** box, select the priority to assign to the contact.

18 If you want to apply the office hours to the e-mail message, click **Will use Office hours**.

19 To close the contact, click **Will Close Contact**.

20 Click **Save**.

--End--

Variable definitions

Variable	Value
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. 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

Rules can be enabled within a rule group.

Procedure steps

Step	Action
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**.

--End--

Disabling a rule

Rules can be disabled within a rule group. You can disable the rule functionality without deleting the rule.

Procedure steps

Step	Action
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**.

--End--

Deleting a rule

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.

Prerequisites

- Create a rule.

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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 **Save**.

--End--

Creating or changing rule groups

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
1	In the Contact Center Manager Administration application, click **Multimedia**.
2	In the left column, click **E-mail**.
3	Click **Rule Groups**.
4	In the **Name** box, type the name of the new rule group. **OR** In the **Rule Groups** list, select the rule group to change.
5	Select the **Matching Type** for the rule group.

6 To add a new rule to the group, click the plus sign (+) button.

7 To remove a rule from the group, click the minus sign (—) button.

8 Configure the new rule using the input criteria, responses, and general settings.

9 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.

10 Click **Save**.

--End--

Variable definitions

Variable	Value
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

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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 **Open Duration** 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, 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**.

--End--

Variable definitions

Variable	Value
Open Duration	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 e-mail message for identification and is known as the Subject line classifier. For more information, see the Subject line classifier table below.
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 that you search for keywords if you enabled the keyword search in the body of the e-mail message.

Procedure job aid

Outgoing E-mail messages – Subject line classifiers

When email messages are sent from Avaya Aura™ Contact Center, certain text is inserted into the subject field in order for Avaya Aura™ Contact Center to classify any potential responses. Some of these classifiers are controllable by user settings, others are essential for the operation of Avaya Aura™ Contact Center.

The following table identifies these classifiers:

Subject line classifier table

Classifier Tag	Acronym	Can be disabled?	Description
[<AX-CustomerID>]	Agent Transfer	No	When an agent transfers a contact to an external e-mail address, this tag is inserted into the subject of the outgoing e-mail. When the response arrives from the external party, this tag identifies the conversation thread to re-open for the agent.
[<AD-CustomerID>]	Agent Desktop	Yes	This tag is inserted to distinguish e-mail messages which originated from the Agent Desktop. All agent initiated e-mail messages or responses to customer e-mail messages will include this tag if enabled.
[<AR-CustomerID>]	Auto Response	No	This tag is inserted into all auto-responses sent by AACC. This is done to ensure that a customer reply to an auto-response is routed to an agent rather than potentially getting a further auto-response. Furthermore it ensures that out-of-office and auto-response loops do not occur.
[<ContactID>]	N/A	Yes	This tag is inserted into agent originated e-mail messages or those in response to customer e-mail messages, if enabled. The purpose of this tag is to identify the specific thread any future response from the customer relates to.

Changing the character encoding for outgoing e-mail

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.

Prerequisites

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

Procedure steps

Step **Action**

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.

--End--

Changing the character encoding of e-mail replies

The Email Manager uses the original character set of the inbound e-mail for agent replies. For example, if an agent receives an e-mail message encoded in UTF-8, the agent reply is also encoded in UTF-8. However, if the original e-mail message is encoded with the Latin 1 character set (ISO-8859-1), an option is available to reply in Latin 9 (ISO-8859-15).

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
1	In the Contact Center Manager Administration application, click **Multimedia**.
2	In the left column, click **E-mail**.
3	Click **General Settings**.
4	Under **Customer Replies**, select the **Reply to Latin 1 as Latin 9** check box.
5	Click **Save**.

--End--

Selecting the outgoing e-mail address

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.

Prerequisites

- Configure the e-mail mailbox from which to send outbound e-mail messages. See Creating or changing a recipient mailbox (page 326).
- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Barring e-mail addresses

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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	Type the e-mail address to block, and then click **Save**. *The address appears in the list of Barred Addresses.*
7	Click **Save.**

--End--

Deleting a barred e-mail address

Remove a blocked e-mail address from the barred e-mail address list.

Prerequisites

- 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.

Procedure steps

Step	Action
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.

--End--

Configuring Microsoft Exchange 2007 for sending outgoing e-mail

If Microsoft Exchange 2007 is installed on your e-mail server, configure it to send outgoing e-mail from the Contact Center Multimedia agent desktops.

If you use Microsoft Exchange 2003, additional configuration is not required.

Prerequisites

- Ensure that you use Microsoft Exchange 2007 on your e-mail server.
- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
1	In the Contact Center Manager Administration application, click **Multimedia**.
2	In the left column, click **General Administration**.
3	Click **Server Settings**.
4	Select the **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 Exchange 2007 server.
10	Open the Exchange Management Console.
11	Click **Server Configuration**, **Hub Transport**, **Receive Connectors Tab**.
12	Right-click **Default <Servername>** and click **Properties**.
13	Click the **Authentication** tab.
14	Disable all authentication except • Basic Authentication • Exchange Server Authentication • Integrated Windows Authentication
15	Close the Exchange Management Console.

--End--

Enabling SSL on the Email Manager

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 untrusted or you that are using a test certificate must enable SMTP Authentication on your e-mail server.

Prerequisites

- 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.

Procedure steps

Step	Action
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
```

--End--

Enabling SMTP Authentication on your e-mail server

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 steps

Step	Action
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**.

--End--

Determining if SMTP Authentication is enabled

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 steps

Step	Action
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
```

Attention: 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.

--End--

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 (page 365)
- Adding a voice mail mailbox (page 366)

Configuring a route point for a voice mail skillset

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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 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**.

--End--

Variable definitions

Variable	Value
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 mailbox

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.

Prerequisites

- Configure a skillset for a voice mail contact.
- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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, chose 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**.

--End--

Variable definitions

Variable	Value
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.
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.

Variable	Value
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.

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 (page 369)
- Adding a fax mailbox (page 370)
- Configuring reply addresses (page 372)

Configuring a route point for a fax skillset

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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 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**.

--End--

Variable definitions

Variable	Value
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 mailbox

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.

Prerequisites

- Configure a skillset for a fax contact.
- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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, chose 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**.

--End--

Variable definitions

Variable	Value
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.
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.

Configuring reply addresses

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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 STMP Authentication** check box.
11	In the **Username** box, type the alternative user name.
12	Click **Save**.

--End--

Variable definitions

Variable	Value
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.
Use Alternative username for STMP Authentication	If SMTP authentication is required for your outbound e-mail server, select the user name for the authentication.

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 (page 375)
- Adding a scanned document mailbox (page 376)
- Configuring reply addresses (page 378)

Configuring a route point for a scanned document skillset

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Variable definitions

Variable	Value
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 scanned document mailbox

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.

Prerequisites

- Configure a skillset for a scanned document.
- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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, chose a priority for contacts received in this mailbox.

11 Click **Save**.

--End--

Variable definitions

Variable	Value
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.
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.

Configuring reply addresses

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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 the e-mail server password.
10	To use a different user name for the SMTP authentication, select the **Use Alternative username for STMP Authentication** check box.
11	In the **Username** box, type the alternative user name.
12	Click **Save**.

--End--

Variable definitions

Variable	Value
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.
Use Alternative username for STMP Authentication	If SMTP authentication is required for your outbound e-mail server, select the user name for the authentication.

SMS 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 a SMS skillset (page 382)
- Adding an SMS mailbox (page 382)
- Configuring reply addresses (page 384)

Configuring a route point for a SMS skillset

Configure a route point for an SMS skillset to route SMS contacts to an agent. Skillsets are used to assign the contacts to agents.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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 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**.

--End--

Variable definitions

Variable	Value
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 mailbox

Add an SMS mailbox to the multimedia configuration for receiving Short Message Service (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.

Prerequisites

- Configure a skillset for an SMS contact.
- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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, chose 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**.

--End--

Variable definitions

Variable	Value
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.
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.

Configuring reply addresses

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 a SMS.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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 STMP Authentication** check box.
11	In the **Username** box, type the alternative user name.
12	Click **Save**.

--End--

Variable definitions

Variable	Value
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.
Use Alternative username for STMP Authentication	If SMTP authentication is required for your outbound e-mail server, select the user name for the authentication.

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 might commonly be 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.

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 development Web server name (page 388)
- Configuring welcome messages and text chat labels (page 389)
- Configuring customer notification log (page 390)
- Configuring contact timers (page 391)
- Creating automatic phrases (page 392)
- Deleting an automatic phrase (page 393)
- Creating a page push URL (page 394)

- Deleting a page push URL (page 394)
- Creating Web On Hold URLs groups (page 395)
- Changing the sequence of a Web On Hold group (page 396)
- Deleting a URL from a Web On Hold group (page 396)
- Deleting a Web On Hold group (page 397)

Assigning development Web server name

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.

Prerequisites

- Know the name of your development Web server and the production Web server.

Procedure steps

Step	Action
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, double-click **External Web Server**.
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**.

--End--

Variable definitions

Variable	Value
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

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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.
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**.

--End--

Variable definitions

Variable	Value
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 customer notification log

Configure the customer notification log information to prepare to send an e-mail to the customer of the written conversation.

Prerequisites

- 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.

Procedure steps

Step **Action**

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**.

--End--

Configuring contact timers

Configure the contact timers for Web communications conversations in your Contact Center.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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	Click **Save**.

--End--

Variable definitions

Variable	Value
Message Refresh	The refresh time for the Agent Desktop.
Keep Alive	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.

Creating automatic phrases

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 an 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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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.

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**.

--End--

Deleting an automatic phrase

Delete the automatic phrase to remove it from the list of automatic phrases available to the agents in the Agent Desktop.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
1	In the Contact Center Manager Administration application, click **Multimedia**.
2	In the left column, click **Web Comms**.
3	Click **Auto Phrases**.
4	In the **Auto Phrases** dialog box, select the skillset for which you want 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**.

--End--

Creating a page push URL

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Deleting a page push URL

Delete a page push URL to remove it from the list of pages the agent can push to customers during a Web communications contact.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action

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**.

--End--

Creating Web On Hold URLs groups

Web on hold 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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
1	In the Contact Center Manager Administration application, click **Multimedia**.
2	In the left column, click **Web Comms**.
3	Click **Web On Hold Urls**.
4	Under **Edit Web on Hold URLs**, click **New**.
5	In the **Tag** box, type a name for the new Web on hold group.
6	In the **Description** box, type a description for the Web on hold URL.
7	In the **Hold Time** box, type the number of seconds to display each URL in the customer's browser.

8	In the **Sequence** box, type a number, from 1 to 25 to indicate the URL sequence you are configuring.
9	In the **URL** box, type the URL to display on the customer's Web browser.
10	Click **Add**.
11	Repeat steps 5 to 10 to add all URLs to the current Web on hold group.
12	Click **Save**.

--End--

Changing the sequence of a Web On Hold group

Change the order in which Web pages in a Web on hold group appear to customers.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
1	In the Contact Center Manager Administration application, click **Multimedia**.
2	In the left column, click **Web Comms**.
3	Click **Web On Hold Urls**.
4	Under **Edit Web on Hold URLs**, select the **Tag** to change.
5	Click **Edit**.
6	In the **Sequence** box, type a number, from 1 to 25 to indicate the URL order in the sequence you are configuring.
7	Click **Save**.

--End--

Deleting a URL from a Web On Hold group

Delete a URL from a Web on hold group if the URL is not available.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action

1. In the Contact Center Manager Administration application, click **Multimedia**.
2. In the left column, click **Web Comms**.
3. Click **Web On Hold Urls**.
4. Under **Edit Web on Hold URLs**, click **Edit**.
5. Under **Edit Web On Hold URL Group** dialog box, in the **URLs in Group** box, select the URL to delete.
6. Click **Remove**.
7. Click **Save**.

--End--

Deleting a Web On Hold group

Delete a Web-on-hold group to avoid displaying the Web pages to the customer during Web communications contacts.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
1	In the Contact Center Manager Administration application, click **Multimedia**.
2	In the left column, click **Web Comms**.
3	Click **Web On Hold Urls**.
4	Under **Edit Web on Hold URLs**, select a web on hold group.
5	Click **Delete**.
6	Click **Save**.

--End--

Web communications customer interface configuration

If you use Web communications in your contact center, you can use the Sample Customer Interface (CI) Web site implementation to help you develop pages for your corporate Web site. The Web services architecture is a platform-independent interface that customers can access from both Microsoft .NET and Java applications. Customer Web sites or third-party applications use the open interface for integration with the Contact Center Multimedia system.

In development, you can access the Web services from either ASP.NET or JSP Web applications.

The Customer Interface Web services provide a range of methods to perform the following functions:

- register new customers in the Contact Center Multimedia database
- log on or log off existing customers
- update customer logon credentials
- create customer contacts
- update customer details
- read customer information
- review a customer contact history
- request immediate or scheduled callback requests
- read a contact
- create and maintain a Web communications chat session

For developers who want to integrate with the Contact Center Multimedia system using Web Services, the following items are available on the Avaya Developer Partner Program Web site:

- Web Service documentation including an API reference in HTML format
- an installation package for the Sample Customer Interface Web site

You can use the sample implementation as a reference to help you develop a live customer Web site.

This section contains the following topics:

- functionality and .jsp pages available in the reference implementation
- customizable settings for the Sample Customer Interface

- steps to test the customer interface Web site

Navigation

- Using the sample customer interface Web site (page 400)
- Configuring properties for the sample customer interface Web site (page 409)
- Testing the customer interface Web site (page 411)
- Creating a test customer (page 411)
- Testing request text chat (page 412)
- Testing the request callback (page 413)
- Testing e-mail from Web pages (page 414)

Using the sample customer interface Web site

Use the sample Customer Interface (CI) Web site to demonstrate the basic functions available through the Web services and to test the Contact Center Multimedia in a lab environment.

Prerequisites

- You must create customer user names in the format of a valid e-mail address, such as user@avaya.com. You must use valid user names to test the sample CI Web site and to deploy custom Web sites.
- Create scheduled callbacks with an outbound skillset (OB_) as scheduled callback contacts are licensed under the outbound license. Agents must have an Outbound license to originate a call to a customer.
- You must convert the time to the local time for the customer who receives the outbound call. The time displayed on Contact Center Manager Administration is in Greenwich Mean Time (GMT).
- The To address of an e-mail message must be a recipient mailbox configured in Contact Center Multimedia Administrator.
- The EM_Default_Skillset must have an outgoing e-mail address mapped in the Multimedia Administrator for password reminder requests from the sample CI Web site.

Procedure steps

Step	Action
1	Access the sample CI Web site using the URL: http://<webserver>:8080/CI_Sample_Website;

<webserver> is the host name of the Web server where you installed the sample CI Web site.

Attention: The default port for Apache Tomcat server is 8080. For information about changing the default port, see the Apache Tomcat documentation.

2 View the sample CI Web site pages to understand how the CI web site functions.

--End--

Procedure job aid

Pages and functions available in the sample CI Web site

Page	Function	Notes
registerNewCustomer.jsp	New customers can register their contact information in the Contact Center Multimedia database.	Customers can enter their title, first name, last name, e-mail address, password, postal address, and phone number. When the form is submitted, the information is passed to registerNewCustomer_WSClient.jsp, which invokes the registerNewCustomer Web method to create the new customer in the Contact Center Multimedia database.
loginCustomer.jsp	Existing customers can enter their user name and password to log on.	When the form is submitted, the user name and password are passed to loginCustomer_WSClient.jsp, which invokes the customerLogin Web method. If the customerLogin method returns an error code indicating that the customer is already logged on, and then the customerAlreadyLoggedIn.jsp page is displayed. If the customer chooses Yes to continue, then the loginCustomer_WSClient.jsp is loaded again with the forceLogoff parameter equal to True. The page logs off the customer using the CustomerLogoff Web methods and then logs on the customer again using the CustomerLogin Web method. The customerLogin Web method returns a session key if the customer logs on successfully. The session key is required to call other Web methods for the customer, so it is stored as a session variable that can be used by other .jsp pages in the sample CI Web site. When the customer logs on to the Web site, the sample page appears. Customers use the opening page to request a text chat, a callback, or an e-mail message from the contact center.

Pages and functions available in the sample CI Web site

Page	Function	Notes
logoffCustomer.jsp	This page contains the user name and Logoff button and is used to log off existing customers.	When the form is submitted, the user name is passed to the page logoffCustomer_WSClient.jsp, which invokes the customerLogoff Web method to log the customer off the Web site.
readCustomerDetails_WSClient.jsp	Existing customers can add or edit details in their contact information.	When the customer adds or updates information and clicks Update Details, the form is passed to updateCustomer_WSClient.jsp, which invokes the Web methods updateCustomer, updateAddress, updateEmailAddress, and updatePhoneNumber. If the information in the fields is new, updateCustomer_WSClient.jsp invokes the Web methods addAddress, addEmailAddress, and addPhoneNumber. The results of the updates appear in the updateCustomer_WSClient.jsp page.
updateCustomerLogin.jsp	Existing customers can change their user name and password.	When the form is submitted, the old password and new password are passed to updateCustomerLogin_WSClient.jsp, which invokes either the updateUsername or updatePassword Web method, depending on the information the customer updates.

Pages and functions available in the sample CI Web site

Page	Function	Notes
readCustContactHist_WSClient.jsp	Existing customers can display their contact history and view the last 20 contacts associated with a customer.	The customer can navigate blocks of 20 contacts by using the navigation arrows above the contact history. You can configure the number of contacts displayed on this page by modifying the NO_OF_CONTACTS_TO_DISPLAY property in the web.xml file in the webapps\CI_Sample_Website|WEB_INF folder. This page uses one of four web methods to retrieve the correct block of contacts: • ReadFirstBlockOfContacts • ReadLastBlockOfContacts • ReadNextBlockOfContacts • ReadPreviousBlockOfContacts The Web method that is called is controlled by the parameter pageControl which can have the value of first, last, next, or previous, depending on the navigation arrow the customer clicks. Another parameter, startContactID, is called when pageControl is either previous or next to call the Web methods ReadPreviousBlockOfContacts and ReadNextBlockOfContacts, with the correct contact ID used as a starting point. When a customer clicks any contact ID in the history list, the readContact_WSClient.jsp page invokes the readContact Web method to read the contact details from the Contact Center Multimedia database and display the information.

Pages and functions available in the sample CI Web site

Page	Function	Notes
requestTextChat.jsp	Customers can request a text chat session with an agent.	When the customer requests a text chat session, the skillset, subject, and objective are passed to requestTextChat_WSClient.jsp. The requestTextChat_WSClient.jsp page uses the IsSkillsetInService Web method to verify whether the selected skillset is in service before creating the Web communications contact. If the skillset is in service, then the contact is routed to the skillset. The Web contact is created as a new contact in the Contact Center Multimedia database by using the requestTextChat Web method with the createAsClosed parameter equal to False. The customer is directed to the Web communications URL http://<webserver>:8080/WebComms/jsp/index.jsp; <webserver> is the host name of your Web server. The requestTextChat Web method passes the session key of the currently logged on customer and the contact ID of the new Web communication contact to the Web communications URL. The text chat page appears on the customer desktop. For example, your Web communications URL can be http://<webserver>:8080/WebComms/jsp/index.jsp?sessionKey=2qrc3E7a00&contactID=637142 To display the customer text chat window, the customers are redirected to this URL using the session key and contact ID parameters. If the skillset is not in service, then a message appears indicating that the requested skillset is not in service and a closed Web communications contact is created as a record of the customer's attempt to request a text chat. The closed Web contact is created using the RequestTextChat Web method with the createAsClosed parameter equal to True.

Pages and functions available in the sample CI Web site

Page	Function	Notes
requestScheduledCallback.jsp	Customers can request a scheduled callback at a specified date and time from an agent.	The getOutboundSkillsets_WSClient.jsp Web method within this page displays a list of outbound skillsets. The time for the callback appears in the Outbound Campaign tool on Contact Center Manager Administration on the Progress and Results screen. The time appears in Greenwich Mean Time (GMT). When the form is submitted, the Callback Time is converted to milliseconds. This value is stored in a hidden form input variable called callback_time_milliseconds, which is passed along with the values of the other fields to the RequestScheduledCallback_WSClient.jsp page. The RequestScheduledCallback_WSClient jsp page calls the requestScheduledCallback Web method to create the scheduled callback contact in the Contact Center Multimedia database.

Pages and functions available in the sample CI Web site

Page	Function	Notes
requestImmediateCallback.jsp	Customers can request an immediate callback from an agent.	The getOutboundSkillsets_WSClient.jsp page displays a list of outbound skillsets. An immediate callback is treated as a scheduled callback contact with the current Multimedia server date and time entered as the callback date and time. When the form is submitted, the values of the fields are passed to the requestImmediateCallback_WSClient.jsp page, which first verifies whether the chosen skillset is in service using the IsSkillsetInService Web method. If the skillset is not in service, then the scheduled callback contact is created using the requestImmediateCallback and a message appears indicating that the callback request is handled when the skillset is in service. If the skillset is in service, then the scheduled callback contact is created using the RequestImmediateCallback method and the confirmation message appears.
submitHTMLForm.jsp	Customers can submit HTML forms as an e-mail message to an agent.	When this form is submitted, the values of the input fields are passed to sendmail.jsp. The sendmail.jsp page uses the JavaMail libraries and SMTP server (configured during installation) to send an e-mail message to the specified To address using the customer default e-mail account. The values in the Text Field 1, Text Field 2, Choice 1, Choice 2, and Text Area fields in the form are sent in the body of the e-mail message. No CI Web service methods are used to send the HTML form as an e-mail message. You can configure the Contact Center Multimedia rules to route these e-mail messages to a specific skillset based on keywords in the e-mail subject.

Pages and functions available in the sample CI Web site

Page	Function	Notes
passwordReminder.jsp	Customers can enter their e-mail address and retrieve their password to log on to the Web site.	When this form is submitted, the e-mail address entered by the customer is passed to the passwordReminder_WSClient.jsp page. The sendPasswordReminder Web method resets the customer password and sends the customer the password reminder auto-response configured in the Contact Center Multimedia Administrator. The EM_Default_Skillset must have an outgoing e-mail address mapped in the Multimedia Administrator for password reminder requests from the sample CI Web site. You can configure a different skillset for password reminder requests by configuring the PASSWORD_REMINDER_SKILLSET property in the web.xml file in the webapps\CI_Sample_Website\WEB_INF folder. The text of the password reminder is configured in the Contact Center Multimedia Administrator in auto-responses. If the e-mail address entered in the form does not correspond to the e-mail address of an existing customer in the Multimedia database, the customer receives a message indicating that they cannot log on.
loginCustomer_timeout.jsp	If the customer attempts to use the sample pages after a session expires, a session timeout message displays and the customer can log on again.	A customer session on the sample CI Web site times out after 10 minutes of inactivity. You can change the session timeout value in the web.xml file for the sample CI Web site.

Pages and functions available in the sample CI Web site

Page	Function	Notes
Web-on-hold	Web-on-hold automatically displays a Web page or group of Web pages to customers while they are waiting for an agent to begin their text chat.	You can define the length of time that each URL appears on the customer Web browser. You can use business logic (such as region of customer or time of year) to program which Web-on-hold page or group of pages to display to various users. When the agent joins the conversation, the Web-on-hold page is replaced and the session is in progress.
Text chat frame	The text chat frame displays a complete record of the current chat conversation between an agent and a customer.	Only four or five lines of text are visible in the frame, but you can scroll up or down to view the entire text of the conversation. The frame displays the URL of any pages viewed or pushed by the agent or the customer.

Configuring properties for the sample customer interface Web site

Configure properties for the sample customer interface by editing the web.xml file. Various settings are customizable, including host name, port number, and Web site path.

Procedure steps

Step	Action
1	Access the web.xml file for the sample customer interface Web site in the webapps\CI_Sample_Website\WEB_INF folder of the Tomcat Servlet container.
2	Configure the items to customize.
3	Save and close the web.xml file.

--End--

Procedure job aid

Sample customer interface Web site items available for configuration

Item	Description
CCMM_HOSTNAME	The name of the Contact Center Multimedia server on which the customer interface Web services are located.
EMAILSERVER_HOSTNAME	The host name of the e-mail server used to send e-mail using Java mail and Standard Mail Transfer Protocol (SMTP). The sendmail.jsp page uses SMTP to send e-mail messages to a Multimedia recipient address. The e-mail server must be able to relay e-mail messages to an e-mail server configured in Contact Center Multimedia.
PASSWORD_REMINDER_SKILLSET	The value of PASSWORD_REMINDER_SKILLSET is used by the passwordReminder_WSClient.jsp page. Password reminder e-mail contacts are created as closed contacts within this defined skillset. By default, the password reminder skillset is set to EM_Default_Skillset.
WEBCOMMS_HOSTNAME	The host name of the Web server hosting the Web communications application.
WEBCOMMS_PORT	The port number used by the Web communications application. The default value is 8080.
WEBCOMMS_PATH	The URL path used to access the Web communications application. The default path is /WebComms/jsp/index.jsp.
HTML_FORM_TO_ADDRESS	The default To e-mail address on the page submitHTMLForm.jsp. The HTML_FORM_TO_ADDRESS must be a valid Multimedia recipient address.
HTML_FORM_SUBJECT	The default subject on the page submitHTMLForm.jsp. The default subject is HTML Form Submitted from the Web.
HTML_FORM_RESULT_HEADER	The value used as the first line in the body of e-mail messages sent from the sendmail.jsp page. The default body text is Results of HTML Form Submitted from the Web.
TEXT_CHAT_SUBJECT	The default subject displayed on the requestTextChat.jsp page. The default subject is Text Chat Submitted from the Web.
NO_OF_CONTACTS_TO_DISPLAY	The number of contacts to display on the Read Customer Contact History page.
<session-timeout>10</ session-timeout>	The number of minutes before a customer chat session expires on the Customer Interface Web site. If the customer session expires, the customer must log on again. The default value is 10 minutes.

Testing the customer interface Web site

Test the customer interface Web site to verify that the Web site is installed properly. First, go to the Web site. After the home page opens, you must test procedures to ensure the customer interface Web site works:

- creating a customer
- testing request text chat
- testing request callback functionality
- testing e-mail from Web pages

Prerequisites

- You must have at least one Web communications skillset configured and at least one agent configured who can handle contacts with the Web communications skillset.

Procedure steps

Step	Action
1	Start your Web browser from the Tomcat homepage. If you use the default port for the Apache Tomcat server, the url for the Tomcat homepage is http://<webservername>:8080.
2	Confirm that the sample customer interface homepage opens to http://<webservername>:8080/CI_Sample_Website/.

--End--

Creating a test customer

Create a test customer, using a predefined e-mail and phone number, to use with testing procedures on the customer interface Web site.

Prerequisites

- Create an e-mail address and phone number available for the test customer you defined.

Procedure steps

Step	Action
1	Click **Register New Customer**.
2	Enter the **Title**, **First Name**, **Last Name**, **Username**, **Password**, **E-mail Address**, **Confirm Password**, and **Number** for your test customer. You can add other details about the customer.
3	To log on this customer immediately after you create, select the **Login Customer** check box.

OR
Click **Log in Customer** to log on this customer now.

4 In the **Username** box, type the test customer user name.

5 In the **Password** box, type the test customer password.

6 Click **Log on**.

--End--

Testing request text chat

Text request text chat to ensure that a customer can submit chat and a Contact Center agent can receive the Web communications content.

Prerequisites

- Ensure that an agent is configured who has the Web communications skillset and can receive contacts.

Procedure steps

Step	Action
1	Log on the test customer.
2	Log an agent who can handle a Web communications skillset on to the Agent Desktop. Make the agent available to receive contacts.
3	Click **Request Text Chat** to create a text chat contact.
4	In the **Skillset** box, select a skillset that your agent from step 2 is eligible to handle.
5	In the **Subject** box, type a subject for the text chat.
6	Click **Submit**.
7	On the Agent Desktop, confirm that the logged on agent receives the Web communications contact from the test customer.
8	Close the test contact.
9	Log off the test customer.

--End--

Procedure job aid

Various Web communications settings prevent blocked invitations to ensure that customers with limited Internet access can chat with an agent. The following customer settings and processes enable customers and agents to use chat processes effectively:

- The Web Communications Manager relies on the HTTP protocol to transport messages between the agent and customer using Web service read and write calls. Because all traffic goes through port 80, no new ports need to be opened through

the firewall. This means that customers based in corporations with limited Internet access can chat with an agent.

- Initially, a customer is placed in Web-on-hold to wait for an agent to join the call. The customer browser is redirected to a frame-based Web page that displays video and interactive content while the customer waits for the agent. The customer Web browser is redirected to the chat conversation when the agent joins the session.
- Among the exchanged messages, a request can be made to have a Web page pushed to the other party. The message asks the customer or agent to load a URL. The agent and customer loads separate copies of the same URL thus safeguarding privacy by not sharing cookies or personalized pages. In addition, existing controls in place by customer or agent internet access is respected. For example, an agent cannot push sites barred by a contact center IT department to an agent by a customer.
- The capability of many browsers to prevent pop-up windows do not affect the text chat conversations between customers and agents. All pages pushed from the agent to the customer load within the central frame above the text chat conversation and no separate pop-up windows appear.
- As with any Internet connection, it is important for customers and contact centers to maintain current antivirus definitions and antispyware.

Testing the request callback

Test the request callback function to ensure that a customer can submit a request for a callback and that an agent can receive the request.

Prerequisites

- Ensure that an agent is configured who has an Outbound skillset and can receive contacts.

Procedure steps

Step	Action
1	Log on the test customer.
2	Log an agent who can handle an Outbound skillset on to the Agent Desktop**.** Make the agent available to receive contacts.
3	Click **Request Immediate Callback** to create an outbound contact.
4	In the **Skillset** box, select a skillset that the agent from step 2 is eligible to handle.
5	In the **Subject** box, type a subject for the outbound contact.
6	In the **Objective** box, type a summary of the reason for the callback.
7	Click **Submit**.

8	On the Agent Desktop, confirm that the logged on agent receives the outbound contact from the test customer.
9	Close the test contact.
10	Log off the test customer.

--End--

Testing e-mail from Web pages

Test e-mail from Web pages to ensure that a customer can submit an e-mail and that an agent can receive the e-mail.

Prerequisites

- Ensure that an e-mail message box is already configured that assigns e-mail messages to the skillset to which an agent logs on.

Procedure steps

Step	Action
1	Log on the test customer.
2	Log on an agent who can handle an e-mail message skillset on to the Agent Desktop. Make the agent available to receive contacts.
3	Click **Submit HTML Form** to create an e-mail contact.
4	In the **Mail To** box, type an e-mail message to be forwarded to the agent who is logged on.
5	In the **Subject** box, type a subject for the e-mail message.
6	Click **Submit**.
7	On the Agent Desktop, confirm that the logged on agent receives the e-mail message from the test customer.
8	Close the test contact.
9	Log off the test customer.

--End--

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 might commonly be 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 (page 415)
- Creating automatic phrases (page 416)
- Deleting an automatic phrase (page 417)
- Creating a page push URL (page 418)
- Deleting a page push URL (page 419)

Configuring welcome and disconnect messages

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Creating automatic phrases

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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.
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**.

--End--

Deleting an automatic phrase

Delete the automatic phrase to remove it from the list of automatic phrases available to the agents in the Agent Desktop.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Creating a page push URL

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.
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**.

--End--

Deleting a page push URL

Delete a page push URL to remove it from the list of pages the agent can push to customers during an instant message contact.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.
6	In the **URLs in Group** box, select the URL to delete.
7	Click **Remove**.
8	Click **Save**.

--End--

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 Contact Center *Predictive Outbound* (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 (page 421)
- Configuring RTD Multicast settings (page 424)
- Configuring predictive outbound agent scripts (page 425)

Configuring predictive blending settings

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.

Prerequisites

- Create a blending threshold class. For more information, see Contact Center *Predictive Outbound* (NN44400-106).
- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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.

Attention: 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	—
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	—

Threshold class	Notes
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**.

--End--

Variable definitions

Variable	Value
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

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Configuring predictive outbound agent scripts

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.
- Use a browser to verify the URL for the predictive outbound agent script.

Procedure steps

Step	Action
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**.

--End--

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 (page 428)
- Configuring agent access to contacts (page 428)
- Controlling access to e-mail message text (page 429)
- Creating or changing custom fields in Agent Desktop (page 429)
- Deleting a custom field in Agent Desktop (page 430)
- Configuring the active contact timer (page 430)
- Configuring the callback timer (page 431)
- Configuring the callback trunk access (page 432)
- Specifying the attachment size (page 432)
- Configuring Agent Desktop behavior (page 433)
- Configuring the state of the Agent terminal on log off (page 434)
- Configuring hotdesking (page 435)
- Configuring hotdesking in a Citrix environment (page 435)
- Creating or changing a closed reason (page 436)
- Deleting a closed reason (page 437)
- Importing an Active Directory user to CCMM (page 437)
- Creating an expert group (page 438)
- Adding an agent to an expert group (page 439)
- Deleting an agent from an expert group (page 440)
- Deleting an agent from a skillset associated group (page 440)
- Configuring an Auto Launch application (page 441)
- Configuring Intrinsic settings (page 441)

Resetting an agent password

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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 use the default password. **OR** Type the new password in the **New Password** and **Confirm Password** boxes.
6	Click **Save**.

--End--

Configuring agent access to contacts

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Controlling access to e-mail message text

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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. Click **Save**.

--End--

Creating or changing custom fields in Agent Desktop

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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.

--End--

Deleting a custom field in Agent Desktop

Delete a custom field from the Agent Desktop when it is not required.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Configuring the active contact timer

Configure the hours and minutes that you want a contact to remain open on a desktop without activity.

When this time expires, the contact is automatically placed into pending state. The default time in the Contact Center Multimedia configuration is 1 hour (60 minutes). The actual time that the contact can be open on the desktop without activity is 1 hour less than the maximum open duration for contacts as defined on Contact Center Manager Server.

The default maximum open duration on the Contact Center Manager Server is 1 hour.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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 number of hours and minutes that you want contacts to be active before they move to pending state.

--End--

Configuring the callback timer

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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.

--End--

Configuring the callback trunk access

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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.

--End--

Specifying the attachment size

Specify the maximum size of the attachments that an agent can attach to an e-mail message.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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 that each file can be.

--End--

Configuring Agent Desktop behavior

You can configure the Agent Desktop behavior to alert the agent when a new contact arrives. The behaviour 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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Variable definitions

Variable	Value
New Contact Presentation	The method in which contacts are presented: • Bring to front: The Agent Desktop moves to the front upon arrival of a new contact. If Bring to front is disabled while Give focus is enabled, the Agent Desktop makes a warning sound and the toolbar flashes, but it is not brought to the front. • 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

Configure the agent terminal to be in idle or busy state when the agent logs off of the Agent Desktop.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Configuring hotdesking

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.

Prerequisites

- Install Contact Center Multimedia or Agent Desktop. See *Avaya Aura™ Contact Center Installation* (NN44400-311).
- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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.

--End--

Configuring hotdesking in a Citrix environment

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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.

--End--

Creating or changing a closed reason

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 (page 436)

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.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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 **Closed Reason**, type a name for the **Closed Reason**.
5	Specify a type of contact for each closed reason.
6	Under **Default Closed Reasons** box, beside **E-mail**, select the configured closed reason to apply to e-mail messages by default.
7	Under the **Default Closed Reasons** box, beside **Web Comms**, select the configured closed reason to apply to Web communications contacts by default.

--End--

Configuring default closed reasons

You can specify a default closed reason for each contact type (e-mail, fax, SMS, Web comms, Scanned doc, 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.

Prerequisites

- create a closed reason. See Creating or changing a closed reason (page 436).

Procedure steps

Step	Action
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	Select a closed reason for each contact type.
5	Click **Save**.

--End--

Deleting a closed reason

Delete a closed reason if you do not want the reason to appear in the Agent Desktop application.

Prerequisites

- Log on to the Contact Center Manager Administration application.

Procedure steps

Step	Action
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**.

--End--

Importing an Active Directory user to CCMM

To add an agent to the Experts list, you must import the agent to CCMM.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.

3 Double-click **Expert Administration**.

4 In the **Expert Administration** window, in the **Connect to AD as** section, type your username and password.

5 In the **Connect to CCMM as section**, type your username and password.

6 Select the agents' names to import.

7 Click **Import**.

The agent name appears in the Experts list.

--End--

Creating an expert group

After you create an experts group, agents in your contact center can consult Instant Experts groups after they log on to Agent Desktop.

Prerequisites

- Log on to CCMM.
- Ensure that you have agent names in the Experts list.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Expert Administration**.
4	In the **Groups** section, click the New button.
5	In the **New Expert Group** dialog box, type the <group name>.
6	Click **OK**.

--End--

Variable definitions

Variable	Value
<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.

Adding an agent to an expert group

After you create an Instant Experts group, add the agents that you require for the group.

Prerequisites

- Log on to CCMM.
- Ensure that you have existing expert groups.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Expert Administration**.
4	In the **Experts** list, click the agent name to add to the experts group.
5	In the **Groups** section, click the required group name.
6	Double-click **Group**.
7	In the **Groups** section, click the Refresh button. The agent name appears in the Contains Experts list.

--End--

Deleting an agent from an expert group

If an agent is no longer available, remove the agent name from the Experts list.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Expert Administration**.
4	In the **Groups** section, click the group name to modify.
5	In the **Contains Experts** section, click the agent name to remove from the group.
6	Under the **Contains Experts** section, click **Remove**.
7	In the **Groups** section, click the Refresh button. In the **Contains Experts** section, the agent name no longer appears.

--End--

Deleting an agent from a skillset associated group

If an agent is no longer available, remove the agent name from a skillset associated group.

Procedure steps

Step	Action
1	In the **Contact Center Multimedia Administrator** window, expand **Contact Center Multimedia**.
2	Expand **Agent Desktop Administration**.
3	Double-click **Expert Administration**.
4	In the **Skillset** list, click the required skillset.
5	In the **Contain Experts** list, click the agent name to remove.
6	Under the **Contains Experts** section, click **Remove**.
7	In the **Skillset** section, click the refresh button. The agent name no longer appears in the Contains Experts list.

--End--

Configuring an Auto Launch application

To authorize agents to enable or disable the Auto Launch Application, configure Auto Launch Application.

Prerequisites

- Log on to CCMM server.
- Ensure that you have the file CCADInstrinsicSettings.xml.

Procedure steps

Step	Action
1	Double-click CCADInstrinsicSettings.xml file.
2	To authorize agents to disable an Auto Launch application, after </IntrinsicDetailsList>, enter <ApplicationForceEditable> true </ApplicationForceEditable>.
3	To restrict agents from editing an Auto Launch application, after </IntrinsicDetailsList>, enter <ApplicationForceEditable> false </ApplicationForceEditable>.

--End--

Configuring Intrinsic settings

Use the Intrinsic Settings page to configure application shortcuts and intrinsics to use while running Agent Desktop.

•

Attention: Voice Contact Intrinsics are supported only in SIP-enabled contact centers.

Prerequisites

- You must use the administration tool on a Contact Center Multimedia server in order to configure intrinsics.

Procedure steps

Step	Action
1	In the Contact Center Manager Administration application, click **Multimedia**.
2	In the left column, click **Agent Desktop Configuration**.
3	Click **Intrinsic Settings**.
4	Under **Application 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.

5 Click **Add** to add more applications.

6 Under **Intrinsics**, configure the intrinsics to display data to the agent. You can configure only one intrinsic to force launch.

7 Click **Add** to add more intrinsics.

8 Select the **Application Force Launch Editable** check box to force an application to start.

9 Select the **Launch Application Internal to AAAD** check box to launch Web-based applications inside Agent Desktop. Only Web-based applications work.

10 Select the **Expand Agent Desktop on Answer** check box to expand an Agent Desktop application when a contact is answered.

11 Select the **Voice Contact Search** check box to search for customer history based on the calling line ID for voice contacts. This feature is available only for SIP based systems.

--End--

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.

Attention: 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 (page 444)
- Archiving by outbound campaign (page 444)
- Archiving by e-mail rule (page 445)
- Archiving by skillset (page 446)
- Archiving by closed reason (page 447)
- Restoring an archive (page 448)
- Recovering from a failed archive or restore (page 448)

Starting the archive utility

Start the archive utility to configure your archiving settings and perform the archive or restore of the Contact Center Multimedia database.

Prerequisites

- Log on to the Contact Center Multimedia server.

Procedure steps

Step	Action
1	Click **Start**, **All Programs**, **Avaya**, **Contact Center**, **Multimedia Server**, **Archive Restore**.

--End--

Archiving by outbound campaign

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.

Prerequisites

- Start the archive utility. See Starting the archive utility (page 444).
- Close the Outbound Campaign Management Tool.

Procedure steps

Step	Action
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 Description or 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**.

--End--

Archiving by e-mail rule

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.

Prerequisites

- Start the archive utility. See Starting the archive utility (page 444).

Procedure steps

Step	Action
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 steps 3 and 4 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 Description or Comments** box, type comments or information about this archive.
8	Under **Archive to Folde**r, 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**.

--End--

Archiving by skillset

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.

Prerequisites

- Start the archive utility. See Starting the archive utility (page 444).

Procedure steps

Step	Action
1	In the archive utility, click the **Archive By Skillset** tab.
1	Under the **Skillset** list, click a skillset to archive. Skillsets in the Skillset list marked with an asterisk are no longer in service.
2	Click the right arrow to move the selected skillset to the list of items to archive.
3	Repeat steps 3 and 4 for each skillset to archive.
4	Under **Contacts Closed on or Before**, click the last date for which you want to archive contacts.
5	To include customer data for the contacts with the selected items, clear the **Delete Archive Customer Data** check box.
6	In the **Archive Description or Comments** box, type comments or information about this archive.
7	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.
8	Click **Archive**.
9	On the Archive Scheduler window, select the start date and time to create your archive.
10	On the calendar, select the date time to create your archive.
11	Click **Close**.

--End--

Archiving by closed reason

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.

Prerequisites

- Start the archive utility. See Starting the archive utility (page 444).

Procedure steps

Step	Action
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 steps 3 and 4 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 Description or 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**.

--End--

Restoring an archive

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.

Prerequisites

- Start the archive utility. See Starting the archive utility (page 444).

Attention: 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.

Procedure steps

Step	Action
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**.

--End--

Recovering from a failed archive or restore

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 steps

Step	Action
1	If an archive or restore fails, examine the archive utility **Warnings** box for the cause.

2 Resolve the reported cause.

3 Click **Resume**.

--End--

Security Fundamentals

Secure the Avaya Aura™ Contact Center Release 6.0/6.1 to enable the user to secure the different applications available.

Navigation

- Simple Network Management Protocol (page 452)
- Event viewer settings (page 452)
- Security template (page 453)
- Event Browser and Alarm Monitor (page 453)
- Logon warning message (CCMA and UCM) (page 453)
- Systems Management Server security file (Multimedia) (page 454)
- Contact Center Manager Server Utility to view events on CCMS (page 454)

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.

Security template

Security is a critical task for all organizations and it is always mandated to secure all networked servers by locking down the server operating system setting and services. You can secure Windows Server 2008 Release 2 by applying a predefined security template either locally to the computer or through a network Group Policy Objects (GPO) instead of securing manually.

Contact Center provides a set of predefined Windows Server 2008 Release 2 security templates that can be deployed quickly to secure the Contact Center suite of application servers.

A set of security templates is available for the Contact Center suite of application servers. You can apply the security template to the defined Contact Center application server to secure the Windows Server 2008 Release 2 and meet the minimum security requirements for the Contact Center application operation.

For more information, see Contact Center *Security Templates User Guide*.

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 (page 100).

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.

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 (page 455)

Securing the Server

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.

Prerequisites

- Ensure the Contact Center application server is running.

Procedure steps

Step	Action
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**.

Attention: 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 **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 services**.
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 services**.

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 **Open Ports and Confirm Applications** window, select the ports to open.

21 To restrict which remote machines connect to the ports listed, in the **Open Ports and Confirm Applications** window, select the specific port.

22 Click **Advanced**, and then select the options that apply to your server.

23 Click **OK**.

24 Click **Next**.

25 In the **Confirm Port Configuration** window, review the Inbound Port Configuration, and 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 operation 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 Review the Audit Policy Summary, and then click **Next**.

35 In the **Internet Information Services** window, click **Next**.

36 In the Audit Policy Section, select **Do not audit**.

37 In the **Select Web Service Extension for Dynamic Content** window, select the extensions that apply to your server.

38 Clear the **Prohibit all other Web service extensions not listed above** check box, and then click **Next**.

39 In the **Select the Virtual Directories to Retain** window, select the virtual directories you want to retain on the selected server, and then click **Next**.

40 In the **Prevent Anonymous Users from Accessing content Files** window, clear the **Deny anonymous users write access to content files** check box, and then click **Next**.

41 Review the IIS Security Settings Summary, and then click **Next**.

42 Save your security policy as an XML file to a location on your server.

43 Click **Next**.

44 In the **Apply Security Policy** window, click **Apply Now**, and then click **Next**.

The security policy is applied–the relevant services are disabled and the Windows firewall blocks relevant ports.

45 Click **Next**.

46 Click **Finish**.

--End--

Managing Security

- Security Fundamentals (page 451)
- Platform Security (page 455)
- Security Template (page 461)

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 (page 462)
- Applying the security template locally on the server (page 463)
- Applying the security template in a network domain (page 464)

Activating the Contact Center security template

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/espl) 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 steps

Step	Action
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.

--End--

Applying the security template locally on the server

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/espl) 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 steps

Step	Action
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.

--End--

Applying the security template in a network domain

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.

Prerequisites

- Download Group Policy Management Console (GPMC) from microsoft.com, and install it on the server.

Procedure steps

Step	Action
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**.

--End--

Common server administration

- Microsoft Windows configuration and management (page 469)
- Simple Network Management Protocol administration (page 475)
- Licensing administration (page 479)
- Contact Center database maintenance (page 485)
- Contact Center server High Availability (page 497)
- Common procedures (page 509)
- Server name or IP address change (page 515)

Microsoft Windows configuration and management

Perform the following procedures to configure settings in Microsoft Windows on your servers.

Navigation

- Managing date and time features (page 469)
- Disabling the Windows time service (page 470)
- Verifying Service Packs (page 470)
- Adding a server to a domain (page 471)
- Configuring the operating system for remote access in a domain (page 472)
- Configuring the operating system for remote access in a workgroup (page 473)

Managing date and time features

Manage the date and time features in Microsoft Windows to avoid potential call processing outages.

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

Procedure steps

Step	Action
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.

Attention: 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**.

--End--

Disabling the Windows time service

Disable the Windows Time service to stop it from running and attempting to synchronize the CCMS server time with a time source and to avoid potential call processing outages.

If the Contact Center Manager Server is in a SIP environment or is the Network Control Center server, you can skip this step.

Prerequisites

- Disable Date and Time features. See Disabling the Windows time service (page 470).

Procedure steps

Step	Action
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.

--End--

Verifying Service Packs

Verify that you have the most recent Service Packs for the Contact Center Manager Server software.

Prerequisites

- 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.

Procedure steps

Step	Action
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 the instructions in *Avaya Aura™ Contact Center Upgrade and Patches* (NN44400-410).

--End--

Adding a server to a domain

Add your Contact Center Manager Server to an existing domain and perform other necessary tasks to ensure that your server works in a domain.

After you install Contact Center Manager Server, you can add your server as a member of an existing domain (stand-alone server only).

Prerequisites

- Install Contact Center Manager Server.
- Ensure that you have domain administrator's privileges, or ask the domain administrator to assign you a domain user account for remote access.
- Disable Windows Time Service (for Contact Center Manager Server is in a domain).

Procedure steps

Step	Action
1	Log on to the server on which you installed Contact Center Manager Server.
2	Right-click **My Computer**.

3	Select **Properties**.
4	In the **System Properties** dialog box, click the **Computer Name** tab.
5	Click **Change**.
6	In the **Computer Name Changes** dialog box, click **Domain**.
7	Type the domain name (you must provide the fully qualified domain name, which includes the prefix and suffix).
8	Click **OK**. A message appears indicating that the server now belongs to the domain that you specified.
9	Type a user name and password to add a machine to the domain.
10	Restart the server when you are prompted to do so.

--End--

Configuring the operating system for remote access in a domain

Configure remote access for your server in a domain to allow technical support to access the server.

Prerequisites

- Add your server to the domain.

Procedure steps

Step	Action
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**.

--End--

Configuring the operating system for remote access in a workgroup

Configure remote access for your server in a workgroup to allow technical support to access the server.

Prerequisites

- Add your server to a workgroup.

Procedure steps

Step	Action
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**.

--End--

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 Event Codes* (NN44400-713).

This chapter describes how to configure the Simple Network Management Protocol for your contact center.

Navigation

- Installing Windows SNMP Service (page 475)
- Selecting CCMS events to be forwarded (page 476)
- Selecting CCMA, CCT, and CCMM events to be forwarded (page 477)
- Configuring the NMS (page 477)

Installing Windows SNMP Service

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 steps

Step	Action
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.

--End--

Selecting CCMS events to be forwarded

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 steps

Step	Action
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).

Attention: 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**.

--End--

Selecting CCMA, CCT, and CCMM events to be forwarded

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 Event Codes* (NN44400-713).

Procedure steps

Step	Action
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.

Attention: 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 steps 7 and 8 for each event that you want added to the list of events to be translated into SNMP traps.

Attention: For a list of recommended events to forward to the Network Management System, see Avaya Aura™ Contact Center Event Codes (NN44400-713).

--End--

Configuring the NMS

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.

For more information about configuring your NMS, see your NMS documentation.

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 will 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.

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

Navigation

- Resetting the grace period (page 479)
- Updating the license file (page 480)
- Changing from Nodal to Corporate licensing (page 481)
- Changing the license manager file on a Contact Center Manager Server (page 482)
- Refreshing your server (page 483)

Resetting the grace period

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.

Prerequisites

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

Procedure steps

Step	Action
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.

--End--

Updating the license file

Update the license file to upgrade Contact Center Manager Server.

Procedure steps

Step	Action
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	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.
8	Click **OK** to close the window.
9	Click **Exit**.

--End--

Changing from Nodal to Corporate licensing

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.

Prerequisites

- 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.

Procedure steps

Step	Action
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.
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.

--End--

Changing the license manager file on a Contact Center Manager Server

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

Prerequisites

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

Procedure steps

Step	Action
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 package to the corporate version.
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.

--End--

Refreshing your server

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.

Prerequisites

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

Procedure steps

Step	Action
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**.

--End--

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 Media Application Server (MAS) statistics. To access MAS-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 should always be backed-up at the same time and stored as a matching or synchronized set. They should 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 (page 486)
- Performing an immediate backup of the database (page 487)
- Scheduling a backup of the database (page 489)
- Recovering a scheduled backup (page 490)
- Restoring a backup (page 491)
- Migrating the database (page 493)
- Configuring Integrated Reporting (page 494)

Creating a backup location

Create a backup location with the correct access permissions on your network.

Prerequisites

- Ensure that you have a user account with full read and write permissions to the location for the database backups.

Procedure steps

Step	Action
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**.

--End--

Variable definitions

Variable	Value
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.
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

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, but backups should be made 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.

Prerequisites

- Create a backup location if you want to use a network location for your backup.
- Know which applications you are to back up.

Attention: The CCT, CCMS and CCMM databases should always be backed-up at the same time and stored as a matching or synchronized set. They should also be restored together to ensure the restored systems have synchronized configuration data.

Procedure steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
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

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.

Prerequisites

- Create a backup location.
- Know which applications you are to back up.

Attention: The CCT, CCMS and CCMM databases should always be backed-up at the same time and stored as a matching or synchronized set. They should also be restored together to ensure the restored systems have synchronized configuration data.

Procedure steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
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

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.

Prerequisites

- Ensure that you view the event in Windows Event Viewer and address the reason why the scheduled backup failed.

Procedure steps

Step	Action
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**.

--End--

Restoring a backup

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.

Prerequisites

- Ensure that you know the location of the backup file.
- Ensure that you know which database to restore.

Attention: The CCT, CCMS and CCMM databases should always be backed-up at the same time and stored as a matching or synchronized set. They should also be restored together to ensure the restored systems have synchronized configuration data.

Procedure steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
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.
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 Email Configuration settings in the CCMM administrator point to the correct attachments folder.

Migrating the database

Migrate the database from one server to another. You can also migrate a database from a previous release to the current release.

Prerequisites

- 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 (page 486).

Procedure steps

Step	Action
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**.

--End--

Variable definitions

Variable	Value
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 Email Configuration settings in the CCMM administrator point to the correct attachments folder.

Configuring Integrated Reporting

To access MAS-Contact Summary reports and Multimedia-Contact Summary reports, configure Integrated Reporting in Database Maintenance utility.

Procedure steps

Step	Action
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 <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 to step.

12 To close the **Database Maintenance** utility, click **Exit**.

--End--

Variable definitions

Variable	Value
<server name>	The display name that depends on the server type: MAS or Multimedia.

Contact Center server High Availability

High Availability supports hot standby resiliency for Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), 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.

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.

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 managed IP addresses (page 498)
- Configuring the standby server (page 500)
- Configuring the notification of automatic switchovers (page 501)
- Configuring manual switchovers (page 502)
- Configuring service monitoring (page 503)
- Configuring automatic switchovers (page 506)
- Monitoring switchover information (page 506)
- Reviewing shadowing (page 507)

Configuring managed IP addresses

A Managed IP address is a virtual IP address that is attached to a network adaptor 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 will attach a Managed IP address to its network interface. The managed IP address will only be assigned to the active server and it is used by all other CC applications and clients to connect to that application. The standby server will only assume 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 steps

Step	Action
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**, if applicable.
7	Click **OK**.

--End--

Variable definitions

Variable	Value
Select Mode	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 will always be assigned the MIP. If a switchover occurs the MIP is assigned to the new Active Server. Agents and other applications are not aware that a switchover has occurred because the IP address does not change. A MIP is only used when the Active and Standby Servers are in the same subnet.
Active Server details	The IP address for the server initially configured in Active mode.
Standby Server details	The IP address for the server initially configured in Standby mode.
Trusted IP address	The IP address of a trusted server that is not likely to go down so that both Active and Standby servers have something to ping regularly to verify the network connection.
Remote Geographic Node(s)	The IP address of the optional Remote Geographic Node.

Configuring the standby server

Configure the standby server for each Contact Center Manager Server, Communication Control Toolkit server or Contact Center Multimedia.

Procedure steps

Step	Action
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**.

Attention: 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.

--End--

Variable definitions

Variable	Value
Select Mode	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

Use the High Availability utility to send e-mail to a configured user.

Prerequisites

- Configure the standby server with automatic switchover. See Configuring managed IP addresses (page 498).
- 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.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server, Communication Control Toolkit, or Contact Center Multimedia is installed.
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 email, 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**.

--End--

Variable definitions

Variable	Value
Email	Enable or disable e-mail notifications.
SMTP	Server The SMTP Server name, this will be automatically verified when saving the data.
Username	E-mail User login name.
Password	E-mail User login password.
Charset	E-mail character set to use.
From Address	E-mail address to send notifications from.
To Address	E-mail address to send notifications to.
Hours	The interval, in hours, when an e-mail will be sent to the configured user if an automatic switchover has occurred.

Configuring manual switchovers

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.

Prerequisites

- Configure the standby server for the Contact Center server (CCT, CCMS, or CCMM) you want to manually switchover. See Configuring managed IP addresses (page 498).

Procedure steps

Step **Action**

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**.

--End--

Configuring service monitoring

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.

For switchover to occur, both the Active and the Standby Servers must have their respective switchover check box ‘s selected, a valid license file and shadowing must be running. If the switchover is not enabled, then all internal monitoring counters are reset and the monitoring restarts.

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.

Prerequisites

- Configure the standby server for each Contact Center server (CCT, CCMS) on which you want to configure automatic switchover. See Configuring managed IP addresses (page 498).

Procedure steps

Step	Action
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 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.

--End--

Variable definitions

Variable	Value
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	Will the service be restarted if it stops.
Start Wait Timer	The time in seconds that service monitor will wait before attempting restart or initiating a switchover to the standby server if this service is not running.
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 automatic switchovers

Configure automatic switchover so if the active server fails or is shut down the standby server will automatically run in its place.

Prerequisites

- Configure the standby server for each Contact Center server (CCT, CCMS, or CCMM) on which you want to configure automatic switchover. See Configuring managed IP addresses (page 498).

Procedure steps

Step	Action
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**.

--End--

Monitoring switchover information

Monitor the switchover information to determine why the automatic or manual switchover occurred.

Procedure steps

Step	Action
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**.

--End--

Variable definitions

Variable	Value
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 automatic switchovers (page 506).

Reviewing shadowing

Review the server status to confirm that the shadowing is occurring between the servers.

Procedure steps

Step	Action
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**.

--End--

Common procedures

This chapter describes the common procedures that you perform to administer your Contact Center software.

Navigation

- Starting or stopping Contact Center applications (page 509)
- Stopping individual services (page 510)
- Starting individual services (page 510)
- Disabling services (page 510)
- Enabling services (page 511)
- Adding a server to a domain (page 512)

Starting or stopping Contact Center applications

Use the System Control and Monitor Utility to start and stop all of the applications in Contact Center.

Prerequisites

Attention: 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 will correct itself within a short time.

Procedure steps

Step	Action
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**.

--End--

Stopping individual services

During some procedures, you must stop one or more Windows services to manipulate a feature or function.

Prerequisites

- Know which server you are working on.
- Know which service or services you must stop.

Procedure steps

Step	Action
1	Click **Start**, **Administrative Tools**, **Services**.
2	In the **Services** window, right-click the name of the service and click **Stop**.

--End--

Starting individual services

During some procedures, you must start one or more Windows services to manipulate a feature or function.

Prerequisites

- Know which server you are working on.
- Know which service or services you must start.

Procedure steps

Step	Action
1	Click **Start**, **Administrative Tools**, **Services**.
2	In the **Services** window, right-click the name of the service and click **Start**.

--End--

Disabling services

During some procedures, you must disable one or more Windows services to manipulate a feature or function.

Prerequisites

- Know which server you are working on.

- Know which service or services you must disable.

Procedure steps

Step	Action
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.

--End--

Enabling services

During some procedures, you must enable one or more Windows services to manipulate a feature or function.

Prerequisites

- Know which server which you are working on.
- Know which service or services you must enable.

Procedure steps

Step	Action
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.

--End--

Adding a server to a domain

Add your Contact Center Manager Server to an existing domain and perform other necessary tasks to ensure that your server works in a domain.

After you install Contact Center Manager Server, you can add your server as a member of an existing domain (stand-alone server only).

Prerequisites

- Install Contact Center Manager Server.
- Ensure that you have domain administrator privileges, or ask the domain administrator to assign you a domain user account for remote access.
- Disable Windows Time Service (for Contact Center Manager Server is in a domain).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server.
2	Right-click **My Computer**.
3	Select **Properties**.
4	In the **System Properties** dialog box, click the **Computer Name** tab.
5	Click **Change**.
6	In the **Computer Name Changes** dialog box, click the **Domain** option.
7	Type the domain name (you must provide the fully qualified domain name, which includes the prefix and suffix).
8	Click **OK**. *A message appears indicating that the server now belongs to the domain that you specified.*
9	Type your administrator user name and password.
10	Restart the server when you are prompted to do so.

--End--

Appendix

- Server name or IP address change (page 515)
- Default login values (page 591)

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.

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

- CCMS server name change (page 515)
- CCMS server IP address change (page 522)
- Co-resident server name change (page 530)
- Co-resident server IP address change (page 542)
- CCMA server name change (page 551)
- CCMA server IP address change (page 559)
- CCT server name change (page 564)
- CCT server IP address change (page 573)
- CCMM server name change (page 576)
- CCMM server IP address change (page 585)

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

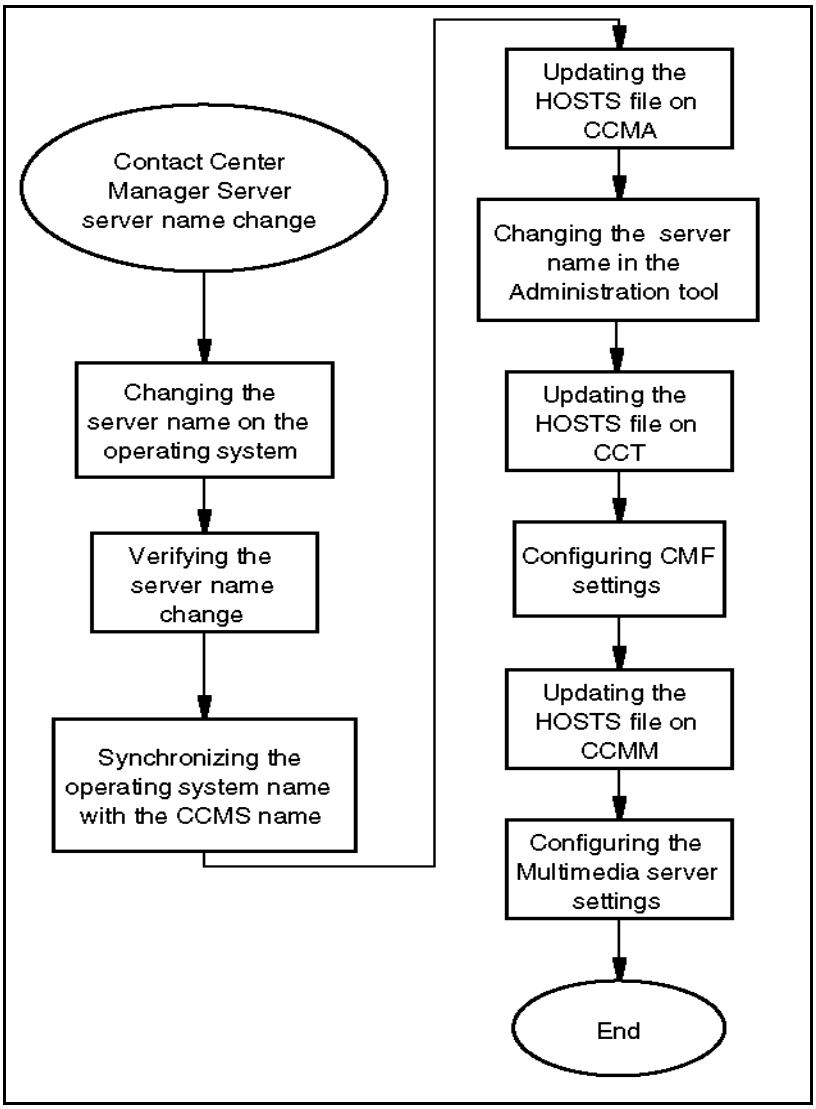
- Ensure that the new server name is unique among both the domain and the other servers on the domain.
- Ensure that the new server name is 6 to 15 characters where the first character is alphabetical.

- Ensure that the new server name contains no underscores (_), spaces ( ), or punctuation.

CCMS server name change procedures

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 (page 516).

CCMS server name change procedures



CCMS server name change navigation

- Changing the server name on the operating system (page 517)
- Verifying the server name change (page 517)
- Synchronizing the operating system name with the CCMS name (page 518)

- Updating the HOSTS file (page 519)
- Changing the server name in the Administration tool (page 519)
- Configuring the Contact Management Framework settings (page 520)
- Configuring the Multimedia server settings (page 521)

Changing the server name on the operating system

Change the server name on the Contact Center Manager Server operating system to reflect the new server name.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server as administrator.
2	On the Contact Center Manager Server, choose **Start**, **Control Panel**, **System and Security**.
3	Under **System**, click **See the name of this computer**.
4	In the **Computer name, domain, and workgroup settings** section, click **Change settings**.
5	Click the **Computer Name** tab.
6	Click **Change**.
7	Type the new server name.
8	Click **OK**.
9	Click **No**.

Attention: 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 (page 518).

10	If you use a Domain Name Service, contact your local network prime to update the DNS with the new server name.

--End--

Verifying the server name change

Verify that the Domain Name Service server or network has the correct server name.

Prerequisites

- Change the server name on the operating system. See Changing the server name on the operating system (page 517).

Procedure steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
server name	The new name of the server.

Synchronizing the operating system name with the CCMS name

Synchronize the operating system name with the Contact Center Manager Server name to ensure that the Contact Center suite uses the new server name.

Prerequisites

- Verify the server name change. See Verifying the server name change (page 517).

Procedure steps

Step	Action
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.

--End--

Updating the HOSTS file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer name to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: 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.

Procedure steps

Step	Action
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 of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Changing the server name in the Administration tool

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.

Prerequisites

- 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 (page 519).

Procedure steps

Step	Action
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**.

--End--

Configuring the Contact Management Framework settings

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.

Prerequisites

- 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 (page 519).
- Know how to restart the CCT server.

Procedure steps

Step	Action
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 **CCT Server**.
5	In the right pane, double-click **CCT Server**.
6	Click the **CMF Configuration** 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.

--End--

Configuring the Multimedia server settings

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.

Prerequisites

- 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 (page 519).

Procedure steps

Step	Action
1	In the Contact Center Manager Administration application, click **Multimedia**.
2	Choose **General Administration**.
3	Click **Server Settings**.
4	Select Contact Center Manager Server.
5	Click **Edit**.
6	In the **Server Name** box, change the name of the Contact Center Manager Server.
7	Click **Save**.
8	When the warning appears describing potential errors for changing this server, click **OK**.
9	If the Contact Center License Manager server is installed on the same server as Contact Center Manager Server, in the **Server Settings** window, click **Contact Center License Server**.
10	Click **Edit**.
11	In the **Server Name** box, type the new name of the Contact Center License Manager server.
12	Click **Save**.
13	If you have a backup Contact Center License Manager server, type the name in the **Backup Server** box.
14	Click **Save**.
15	When the warning appears, click **OK**.

--End--

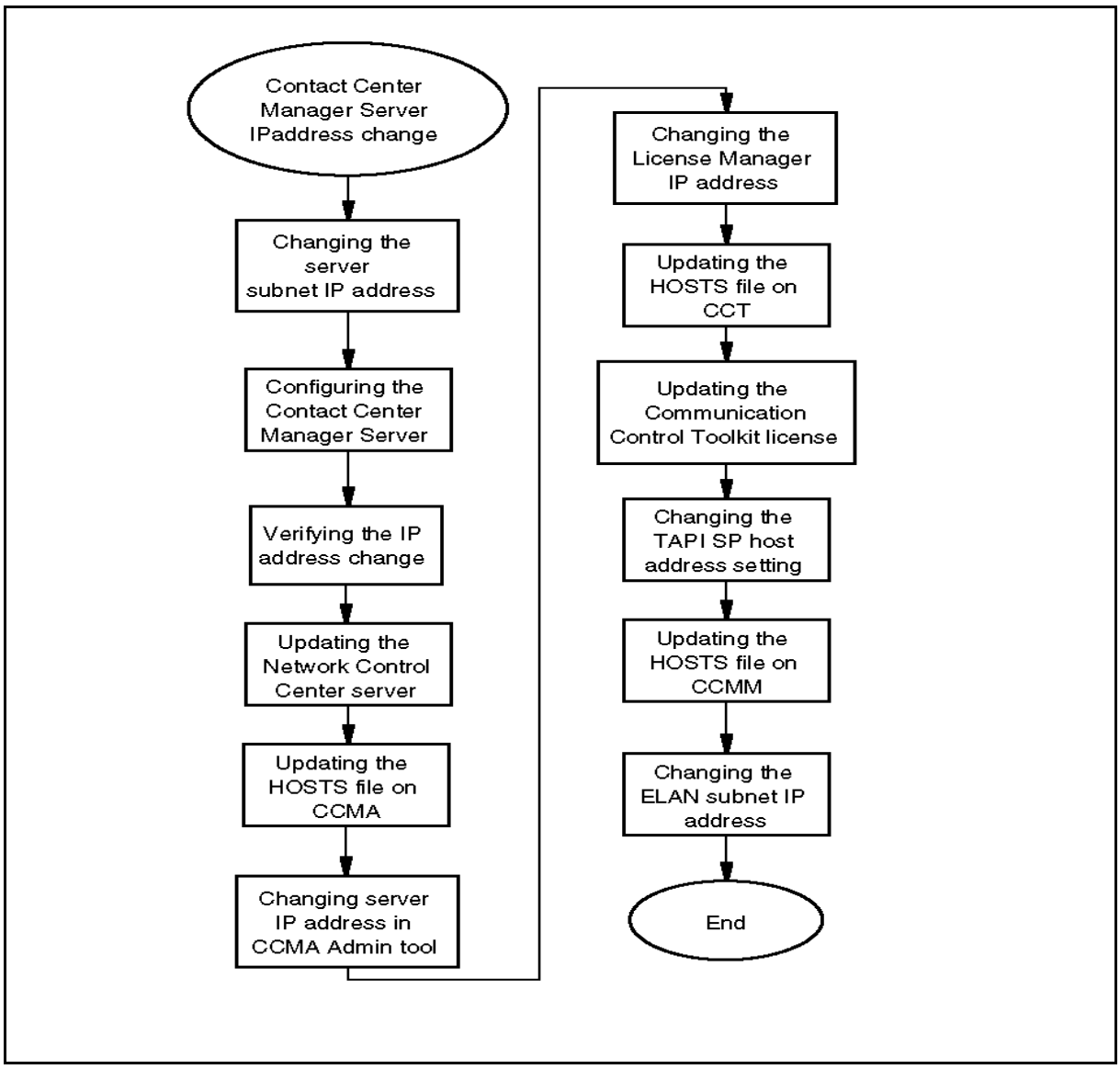
CCMS server IP address change

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

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 (page 523).

CCMS server IP address change procedures



CCMS server IP address change navigation

- Changing the contact center subnet IP address (page 523)
- Configuring the Contact Center Manager Server (page 524)
- Verifying the IP address change (page 524)
- Updating the Network Control Center server (page 525)
- Updating the HOSTS file (page 526)
- Updating the server IP address in CCMA (page 526)
- Changing the Contact Center License Manager IP address (page 527)
- Updating the Communication Control Toolkit license (page 528)
- Changing the ELAN subnet IP address (page 528)

Changing the contact center subnet IP address

Change the contact center subnet IP address where the server IP address is recorded.

Procedure steps

Step	Action
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 Internet, Network 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**.

--End--

Configuring the Contact Center Manager Server

Ensure that the Contact Center Manager Server software has a record of the new IP address for the server to ensure communications between the Contact Center servers continues.

Prerequisites

- Change the contact center subnet IP address. See Changing the contact center subnet IP address (page 523).

Procedure steps

Step	Action
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.

Attention: 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.

--End--

Verifying the IP address change

Verify that the Domain Name Service server or network has the correct server IP address.

Prerequisites

- Configure the Contact Center Manager Server software with the new IP address. See Configuring the Contact Center Manager Server (page 524).

Procedure steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
server name	The name of the Contact Center Manager Server.

Updating the Network Control Center server

Update the Network Control Center server if you have a network of Contact Center Manager Servers connected to a Network Control Center server to ensure the Network Control Center server can identify the Contact Center Manager Server.

Prerequisites

- Ensure that you have a network of Contact Center Manager Servers.
- Verify that the IP address changed. See Verifying the IP address change (page 524).

Procedure steps

Step **Action**

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**.

--End--

Updating the HOSTS file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer IP address to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: 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.

Procedure steps

Step	Action
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 IP address of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Updating the server IP address in CCMA

Update the server IP address to ensure that the Contact Center Manager Server Administration software has a record of the new IP address for the Contact Center Manager Server to ensure communications between the software is maintained.

Prerequisites

- Change the server IP address. See Changing the contact center subnet IP address (page 523).

Procedure steps

Step	Action
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**.

Step	Action
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**.

--End--

Changing the Contact Center License Manager IP address

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.

Prerequisites

- 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 (page 526).

Procedure steps

Step	Action
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**.

--End--

Updating the Communication Control Toolkit license

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.

Prerequisites

- 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 (page 526).

Procedure steps

Step	Action
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 **Licensing** tab.
7	Under **Primary License Manager Server**, in the **IP Address** box, type the new IP address.
8	On the **File** menu, click **Exit**.

--End--

Changing the ELAN subnet IP address

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.

Prerequisites

- Change the contact center subnet IP address. See Changing the contact center subnet IP address (page 523).

Procedure steps

Step	Action
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.

--End--

Co-resident server name change

Change the name 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 other servers in the Contact Center Suite. The new name of the server must meet the specifications of the server names in the Contact Centersuite.

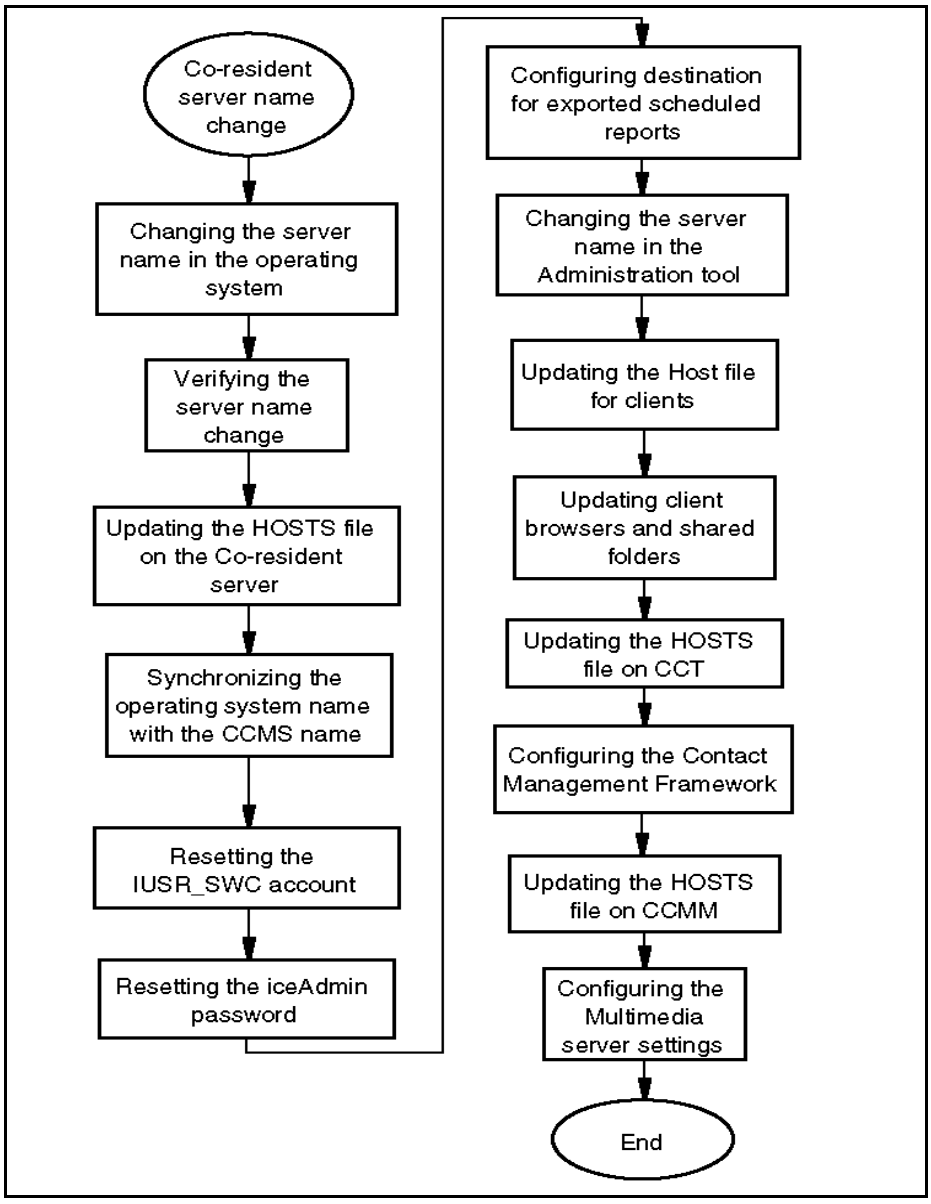
Prerequisites for Co-resident server name change

- 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

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 (page 531).

Co-resident server name change procedures



Co-resident server name change navigation

- Changing the server name in the operating system (page 532)
- Verifying the server name change (page 533)
- Updating the HOSTS file (page 533) on the co-resident server
- Synchronizing the operating system name with the CCMS name (page 534)
- Resetting the IUSR_SWC account (page 534)
- Resetting the iceAdmin password (page 536)

- Configuring destination for exported scheduled reports (page 537)
- Changing the server name in the Administration tool (page 538)
- Updating the HOSTS file for clients (page 539)
- Updating client browsers and shared folders (page 536)
- Updating the HOSTS file (page 533) on CCT
- Configuring the Contact Management Framework (page 539)
- Updating the HOSTS file (page 533) on CCMM
- Configuring the Multimedia server settings (page 540)

Changing the server name in the operating system

Change the server name on the Contact Center Manager Server operating system to reflect the new name of the server.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Server as administrator.
2	On the Contact Center Manager Server, choose **Start**, **Control Panel**, **System and Security**.
3	Under **System**, click **See the name of this computer**.
4	In the **Computer name, domain, and workgroup settings** section, click **Change settings**.
5	Click the **Computer Name** tab.
6	Click **Change**.
7	Type the new server name.
8	Click **OK**.
9	Click **No**.

Attention: 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 (page 534).

10	If you are using a Domain Name Service, contact your local network prime to update the DNS with the new server name.

--End--

Verifying the server name change

Verify that the Domain Name Service server or network has the correct server name.

Prerequisites

- Ensure that you use a Domain Name Service server in your network.

Procedure steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
server name	The new name of the server.

Updating the HOSTS file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer name to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: 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.

Procedure steps

Step	Action
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 of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Synchronizing the operating system name with the CCMS name

Synchronize the operating system name with the Contact Center Manager Server name to ensure that the Contact Center suite uses the new server name.

Prerequisites

- Verify that the server name change. See Verifying the server name change (page 533).

Procedure steps

Step	Action
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**, **Manager Server**, **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.

--End--

Resetting the IUSR_SWC account

Reset the IUSR_SWC account to reflect the new server name to ensure that users log on to the correct Contact Center Manager Server and Contact Center Manager Administration server.

Prerequisites

- Verify that the server name changed. See Verifying the server name change (page 533).

- Obtain the user ID and password for the IUSR_SWC account from your network administrator.

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Choose **Start**, **All Programs**, **Administrative Tools**, **Internet Information Services (IIS) Manager**.
3	In the **Internet Information Services (IIS) Manager** window, expand **<Computer_Name> (local computer)**.
4	Expand the **Web Sites** folder.
5	Right-click **Default Web Site**, and then select **Properties**.
6	In the **Default Web Site Properties** dialog box, click the **Directory Security** tab.
7	In the **Directory Security** tab, under **Authentication and access control**, click **Edit**.
8	In the **Authentication Methods** dialog box, click **Browse**.
9	In the **Select User** dialog box, click **Advanced**.
10	Click **Find Now**.
11	From the list of user accounts, select the IUSR_SWC account, and then click **OK**.
12	Click **OK**.
13	In the **Password** box, type the password you used for this account when you initially configured it.
14	Click **OK**.
15	Type the password again, and then click **OK**.
16	Click **OK** to save your changes.

--End--

Variable definitions

Variable	Value
Computer Name	The name of the computer you must configure for the IIS protocol.

Resetting the iceAdmin password

Reset the iceAdmin password to access the contents of the Administration database.

Prerequisites

- Obtain the domain account name and password from your network administrator.

Procedure steps

Step	Action
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 Passwor**d 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**.

--End--

Updating client browsers and shared folders

Update the client browsers and shared folders to reference the new Contact Center Manager Administration server name in the browser.

Prerequisites

- 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 (page 539).

Procedure steps

Step	Action
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 steps 4 to 10 for each report.

--End--

Variable definitions

Variable	Value
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 destination for exported scheduled reports

Configure the destination for exported scheduled reports if you export scheduled reports to a domain network computer.

Prerequisites

- Plan to export scheduled reports to a computer on your domain network.

Procedure steps

Step	Action
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**.

--End--

Changing the server name in the Administration tool

Change the Contact Center Manager Server name in the Administration tool to ensure that the connections in Contact Center Manager Administration are to the correct server.

Prerequisites

- 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 Manager Administration server with the new Contact Center Manager Server name. See Updating the HOSTS file (page 519).

Procedure steps

Step	Action
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	Double-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**.

--End--

Updating the HOSTS file for clients

If you have no DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer name to ensure that all clients can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your client.

Attention: 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.

Procedure steps

Step	Action
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 name of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Configuring the Contact Management Framework

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.

Prerequisites

- 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 (page 519).
- Know how to restart the CCT server.

Procedure steps

Step	Action
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, click **CCT Server**.
5	In the right pane, double-click **CCT Server**.
6	Click the **CMF Configuration** 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.

--End--

Configuring the Multimedia server settings

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.

Prerequisites

- 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 Multimedia server with the new Contact Center Manager Server name. See Updating the HOSTS file (page 519).

Procedure steps

Step	Action
1	In the Contact Center Manager Administration application, click **Multimedia**.
2	Choose **General Administration**.
3	Click **Server Settings**.
4	Select Contact Center Manager Server.
5	Click **Edit**.
6	In the **Server Name** box, change the name of the Contact Center Manager Server.
7	Click **Save**.

8 When the warning appears describing potential errors for changing this server, click **OK**.

9 If the Contact Center License Manager server is installed on the same server as Contact Center Manager Server, in the **Server Settings** window, click **Contact Center License Server**.

10 Click **Edit**.

11 In the **Server Name** box, type the new name of the Contact Center License Manager server.

12 Click **Save**.

13 If you have a backup Contact Center License Manager server, type the name in the **Backup Server** box.

14 Click **Save**.

15 When the warning message appears, click **OK**.

--End--

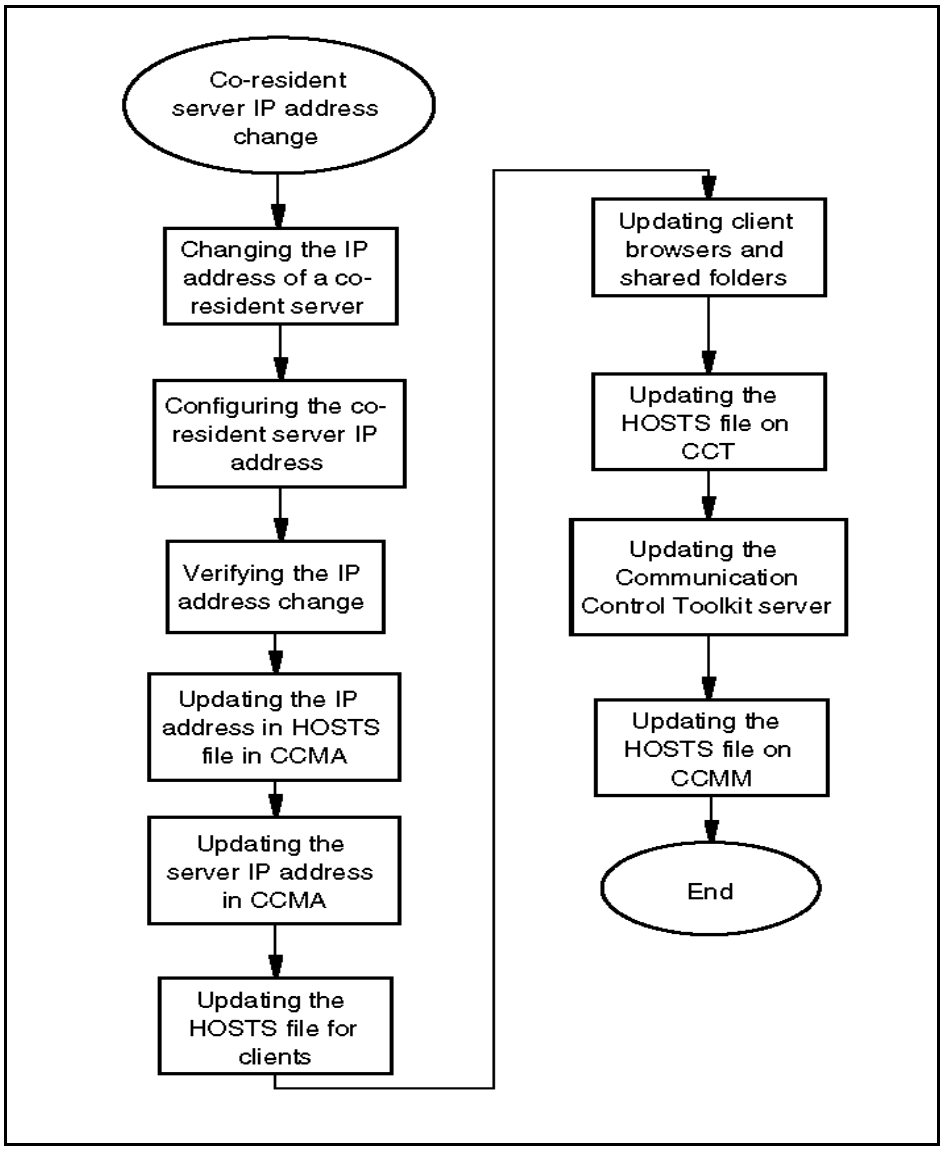
Co-resident server IP address change

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

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 (page 543).

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 (page 543)
- Configuring the co-resident server IP address (page 544)
- Verifying the server IP address change (page 544)
- Updating the Network Control Center server (page 545)
- Updating the HOSTS file (page 545) on CCMA
- Updating the server IP address in CCMA (page 546)
- Updating the HOST file for clients (page 547)
- Updating client browsers and shared folders (page 548)
- Updating the HOSTS file (page 545) on CCT
- Updating the HOSTS file (page 545) on CCMM

Changing the contact center subnet IP address of the co-resident server

Update the server IP address to ensure that the co-resident server address is updated so that all Contact Center servers have a record of the new IP address for the server to ensure communications between the software is maintained.

Procedure steps

Step	Action
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**.

--End--

Configuring the co-resident server IP address

Update the server IP address to ensure that the co-resident server address is updated so that all Contact Center servers have a record of the new IP address for the server to ensure communications between the software is maintained.

Procedure steps

Step	Action
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 **OK**.

--End--

Verifying the server IP address change

Verify that the Domain Name Service server or network has the correct server IP address.

Prerequisites

- Configure the Contact Center Manager Server software with the new IP address. See Configuring the Contact Center Manager Server (page 524).

Procedure steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
server name	The name of the Contact Center Manager Server.

Updating the Network Control Center server

Update the Network Control Center server if you have a network of Contact Center Manager Servers connected to a Network Control Center server to ensure the Network Control Center server can identify the Contact Center Manager Server.

Prerequisites

- Ensure that you have a network of Contact Center Manager Servers.
- Verify that the IP address is changed. See Verifying the IP address change (page 524).

Procedure steps

Step	Action
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**.

--End--

Updating the HOSTS file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer IP address to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: 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.

Procedure steps

Step	Action
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 IP address of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Updating the server IP address in CCMA

Update the server IP address to ensure that the Contact Center Manager Server Administration software has a record of the new IP address for the server to ensure communications between the software is maintained.

Prerequisites

- Change the server IP address. See Changing the contact center subnet IP address of the co-resident server (page 543).

Procedure steps

Step	Action
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**.

--End--

Updating the HOST file for clients

If you have no DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer name to ensure that all clients can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your client.

Attention: 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.

Procedure steps

Step	Action
1	Log on to the client.
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 name of the Contact Center Manager Server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Updating client browsers and shared folders

Update the client browsers and shared folders to reference the new Contact Center Manager Administration server name in the browser.

Prerequisites

- 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 and that you updated the HOSTS file on the clients with the new Contact Center Manager Server name. See Updating the HOST file for clients (page 547).

Procedure steps

Step	Action
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, right-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 steps 4 to 11 for each report.

--End--

Variable definitions

Variable	Value
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].

Changing the Contact Center License Manager IP address

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.

Prerequisites

- Ensure that the Domain Name Service server is updated with the new Contact Center Manager Server IP address or that 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 (page 545).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	From the **Start** menu, click **All Programs**, **Avaya, Contact Center**, **Manager Administration**, **Configuration**.
3	In the right pane, click the **LM Service Configuration** icon.
4	In the **Primary License Manager Server's IP Address** box, type the new IP address.
5	Click **OK**.
6	On the **Configuration Setup Completed** dialog box, click **OK**.
7	Click **Yes** to restart the Contact Center License Manager service.
8	Click **OK**.
9	On the **File** menu, click **Exit**.

--End--

Updating the Communication Control Toolkit server IP address in CCMA

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 steps

Step	Action
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**.

--End--

Updating the Communication Control Toolkit Provider IP address

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 steps

Step	Action
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 **CCT Website: URL**.
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**

--End--

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.

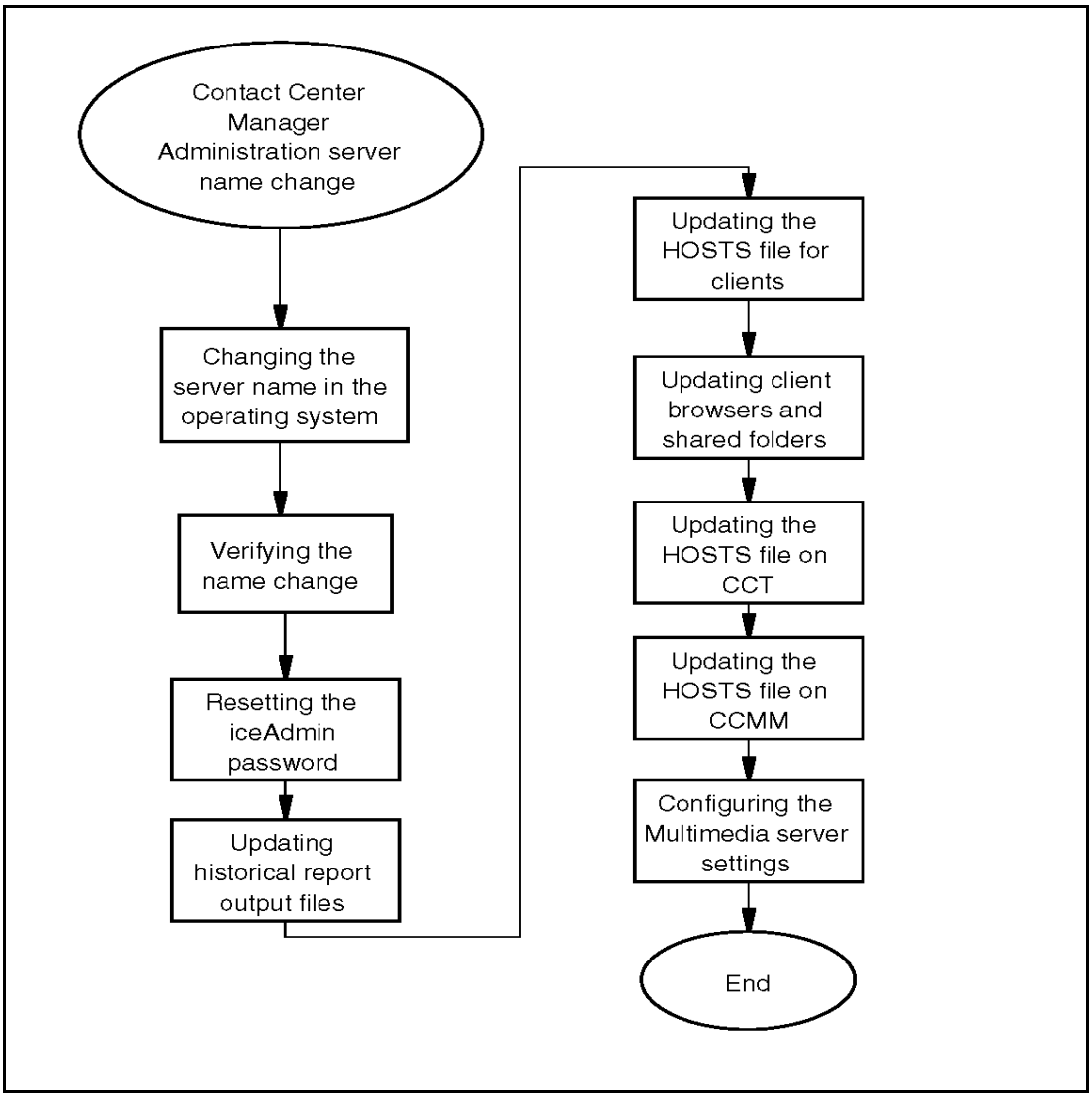
Prerequisites for CCMA server name change

- 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

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 (page 552).

CCMA server name change procedures



CCMA server name change navigation

- Changing the server name in the operating system (page 553)
- Verifying the server name change (page 553)
- Resetting the iceAdmin password (page 554)
- Updating historical report output files (page 555)
- Updating the HOSTS file for clients (page 555)

- Updating client browsers and shared folders (page 556)
- Updating the HOSTS file (page 557) on CCT
- Updating the HOSTS file (page 557) on CCMM
- Configuring the Multimedia server settings (page 558)

Changing the server name in the operating system

Change the name of the Contact Center Manager Administration server in the operating system to indicate the name of the server.

Procedure steps

Step	Action
1	On the Contact Center Manager Administration server, select **Start**, **Control Panel**, and then click **System and Security, 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.

--End--

Verifying the server name change

Verify that the Domain Name Service server or network has the correct server name.

Prerequisites

- Ensure that you use a Domain Name Service server in your network.

Procedure steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
server name	The new name of the server.

Resetting the iceAdmin password

Reset the iceAdmin password to access the contents of the Administration database.

Prerequisites

- Obtain the domain account name and password from your network administrator.

Procedure steps

Step	Action
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 Passwor**d box, reenter the old 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 on 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**.

--End--

Updating historical report output files

Configure the destination for exported scheduled reports if you export scheduled reports to a domain network computer.

Prerequisites

- Plan to export scheduled reports to a computer on your domain network.

Procedure steps

Step	Action
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**.

--End--

Updating the HOSTS file for clients

If you have no DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer name to ensure that all clients can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your client.

Attention: 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.

Procedure steps

Step	Action
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 name of the Contact Center Manager Administration.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Updating client browsers and shared folders

Update the client browsers and shared folders to reference the new Contact Center Manager Administration server name in the browser.

Prerequisites

- 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 (page 555).

Procedure steps

Step	Action
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 steps 4 to 11 for each report.

--End--

Variable definitions

Variable	Value
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

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer name to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: 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.

Procedure steps

Step **Action**

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 of the Contact Center Manager Administration.

5 On the **File** menu, click **Save**.

6	Close all windows.

--End--

Configuring the Multimedia server settings

Configure the Multimedia server settings to ensure that the Multimedia database knows where to find contacts and has the correct name of the Contact Center Manager Server.

Prerequisites

- 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 Contact Center Multimedia server with the new Contact Center Manager Administration name. See Updating the HOSTS file (page 557).

Procedure steps

Step	Action
1	In the Contact Center Manager Administration application, click **Multimedia**.
2	Choose **General Administration**.
3	Click **Server Settings**.
4	Select Contact Center Manager Administration.
5	Click **Edit**.
6	In the **Server Name** box, change the name of the Contact Center Manager Administration.
7	Click **Save**.
8	If a warning appears describing potential errors for changing this server, click **OK**.

--End--

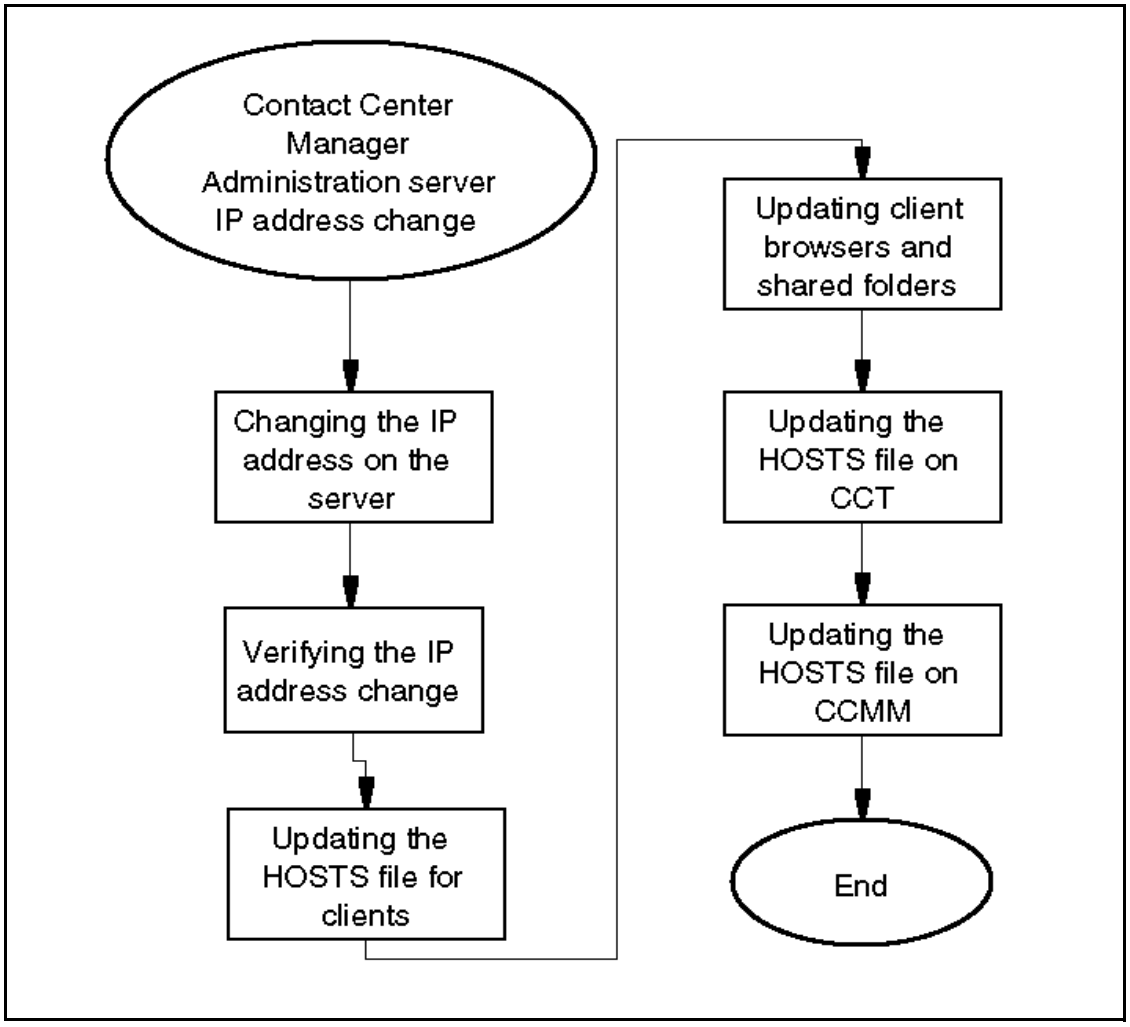
CCMA server IP address change

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

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 (page 559).

CCMA server IP address change procedures



CCMA server IP address change navigation

- Changing the server IP address on the server (page 560)
- Verifying the server IP address change (page 560)

- Updating the HOSTS file for clients (page 561)
- Updating client browsers and shared folders (page 562)
- Updating the HOSTS file (page 563) on the Communication Control Toolkit server
- Updating the HOSTS file (page 563) on the Contact Center Multimediaserver

Changing the server IP address on the server

Update the server IP address to ensure that the Contact Center Manager Administration software has a record of the new IP address for the server to ensure communications between the software is maintained.

Procedure steps

Step	Action
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.

--End--

Verifying the server IP address change

Verify that the Domain Name Service server or network has the correct server IP address.

Prerequisites

- Configure the Contact Center Manager Administration software with the new IP address. See Verifying the server IP address change (page 560).

Procedure steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
server name	The name of the Contact Center Manager Server.

Updating the HOSTS file for clients

If you have no DNS server, you must manually update the HOSTS file on each client in your contact center with the new computer name to ensure that all clients can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your client.

Attention: 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.

Procedure steps

Step	Action
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 name of the Contact Center Manager Administration.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Updating client browsers and shared folders

Update the client browsers and shared folders to reference the new Contact Center Manager Administration server name in the browser.

Prerequisites

- 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 HOST file for clients (page 547).

Procedure steps

Step	Action
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, right-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 steps 4 to 11 for each report.

--End--

Variable definitions

Variable	Value
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

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer IP address to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: 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.

Procedure steps

Step	Action
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 IP address of the Contact Center Manager Administration.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

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.

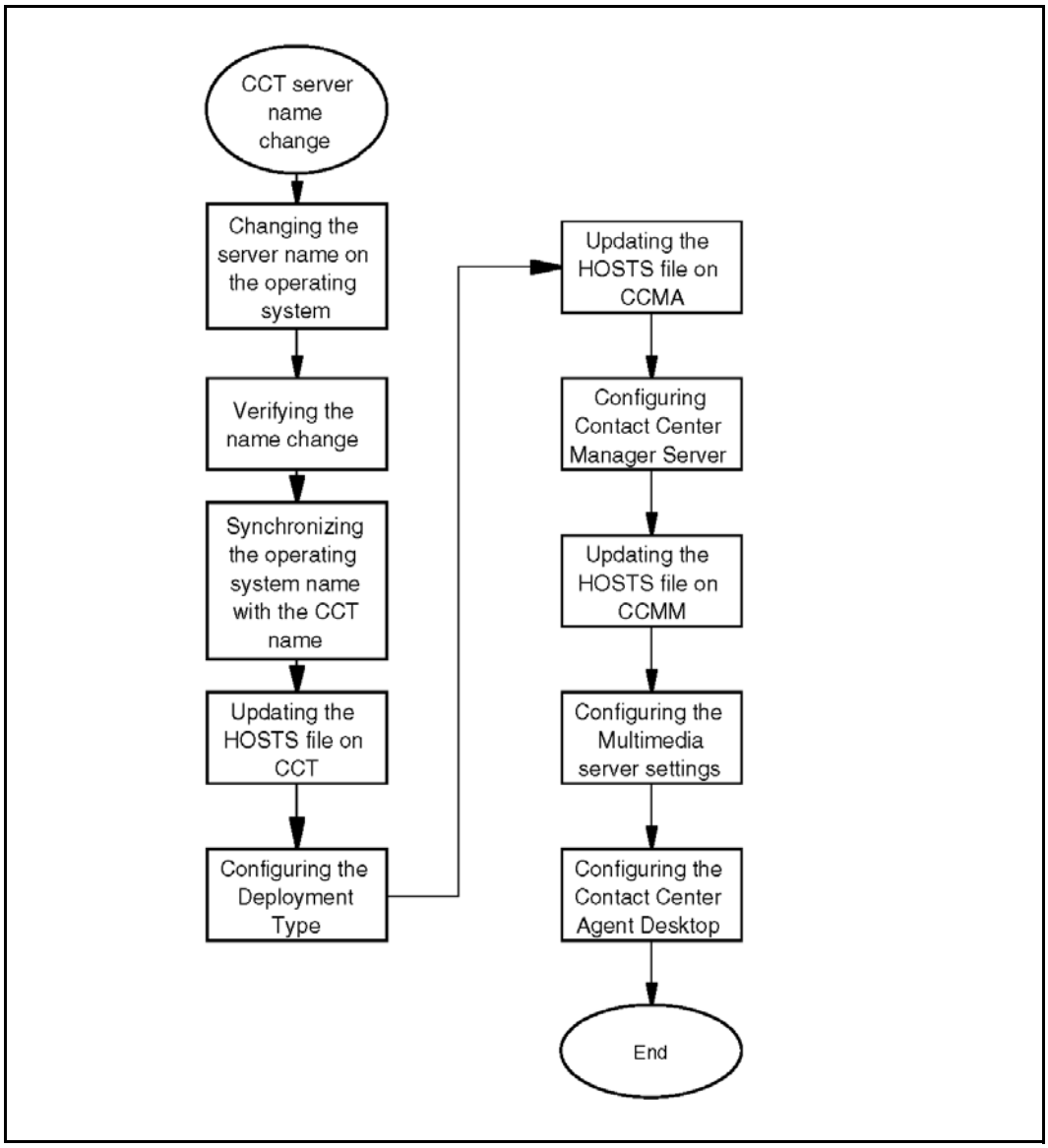
Prerequisites for CCT server name change

- 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

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 (page 565).

CCT server name change procedures



CCT server name change navigation

- Changing the server name on the operating system (page 566)
- Verifying the server name change (page 566)
- Synchronizing the operating system name with the CCT name (page 567)
- Updating the HOSTS file (page 568) on CCT
- Configuring the deployment type for CCT (page 568)
- Updating the HOSTS file (page 568) on CCMA
- Configuring Contact Center Manager Server (page 570)

- Updating the HOSTS file (page 568) on CCMM
- Configuring the Multimedia server settings (page 571)
- Configuring the Agent Desktop (page 571)

Changing the server name on the operating system

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.

Prerequisites

- Know how to restart the Communication Control Toolkit server.

Procedure steps

Step	Action
1	On the Communication Control Toolkit Server, choose **Start**, **Control Panel**, **System and Security**.
2	Under **System**, click **See the name of this computer**.
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**.

Attention: 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 (page 567).

8	If you use a Domain Name Service, contact your local network prime to update the DNS with the new server name.

--End--

Verifying the server name change

Verify that the Domain Name Service server or network has the correct server name.

Prerequisites

- Ensure that you use a Domain Name Service server in your network.

Procedure steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
server name	The new name of the server.

Synchronizing the operating system name with the CCT name

Synchronize the operating system name with the Communication Control Toolkit name to ensure that the Contact Center suite uses the new server name.

Prerequisites

- Verify the server name change. See Verifying the server name change (page 566).

Procedure steps

Step	Action
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 Synchronization Utility box, click **OK**.
7	Restart the server.

--End--

Updating the HOSTS file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer name to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: 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.

Procedure steps

Step	Action
1	Log on to each 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 of the Communication Control Toolkit.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Configuring the deployment type for CCT

Configure the deployment type for the CCT server to manage the contact routing for your network configuration. Update the deployment type in Communication Control Toolkit with the new Communication Control Toolkit server name.

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

Prerequisites

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

- Know how to stop and restart the CCT services.
- Change the name of the Communication Control Toolkit server in the operating system. See Changing the server name on the operating system (page 566).

Procedure steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
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.

Configuring Contact Center Manager Server

Configure the Contact Center Manager Server software with the name of the new Communication Control Toolkit to ensure that Communication Control Toolkit works correctly.

Prerequisites

- Change the name of the Communication Control Toolkit server in the operating system. See Changing the server name on the operating system (page 566)

Procedure steps

Step	Action
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.

--End--

Configuring the Multimedia server settings

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.

Prerequisites

- 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 (page 568).

Procedure steps

Step	Action
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**.

--End--

Configuring the Agent Desktop

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.

Prerequisites

- 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 (page 566).

Procedure steps

Step	Action

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.

--End--

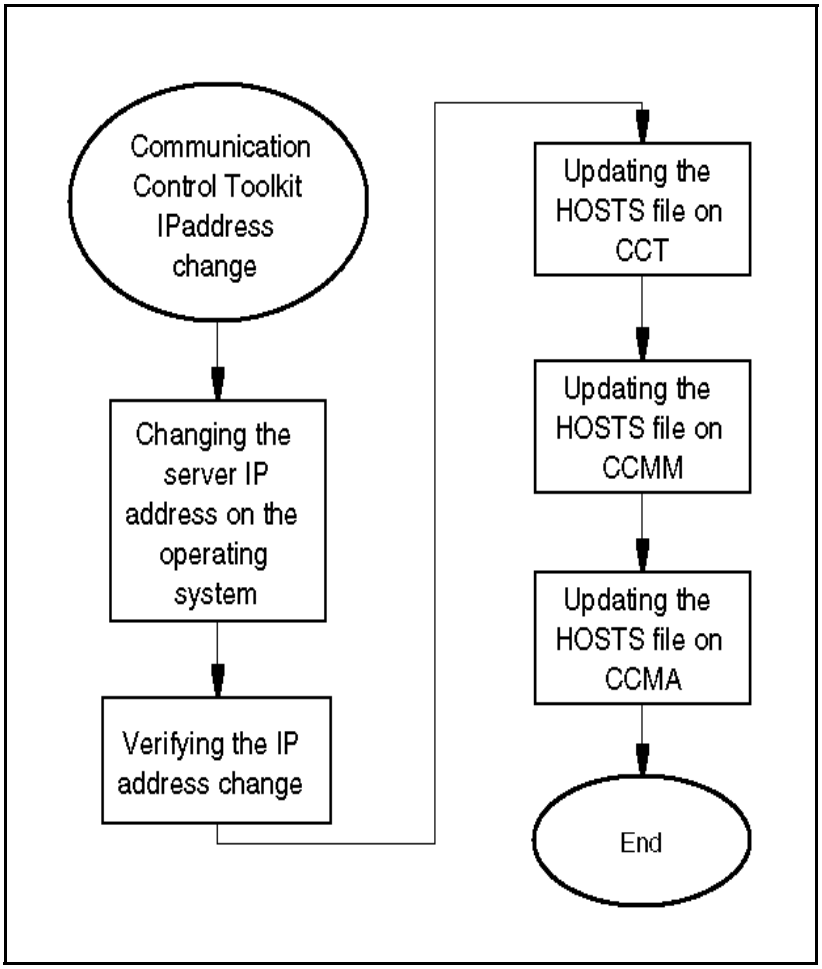
CCT server IP address change

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

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 (page 573).

CCT server IP address change procedures



CCT server IP address change navigation

- Changing the server IP address on the operating system (page 574)
- Verifying the server IP address change (page 574)
- Updating the HOSTS file (page 575) on CCT.
- Updating the HOSTS file (page 575) on CCMM.

- Updating the HOSTS file (page 575) on CCMA.

Changing the server IP address on the operating system

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.

Prerequisites

- Know how to restart the Communication Control Toolkit services.

Procedure steps

Step	Action
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.

--End--

Verifying the server IP address change

Verify that the Domain Name Service server or network has the correct server IP address.

Prerequisites

- Configure the Communication Control Toolkit software with the new IP address.

Procedure steps

Step	Action

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.

--End--

Variable definitions

Variable	Value
server name	The name of the Communication Control Toolkit server.

Updating the HOSTS file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer IP address to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: 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.

Procedure steps

Step **Action**

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 IP address of the Contact Center Manager Server.

5 On the **File** menu, click **Save**.

6 Close all windows.

--End--

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.

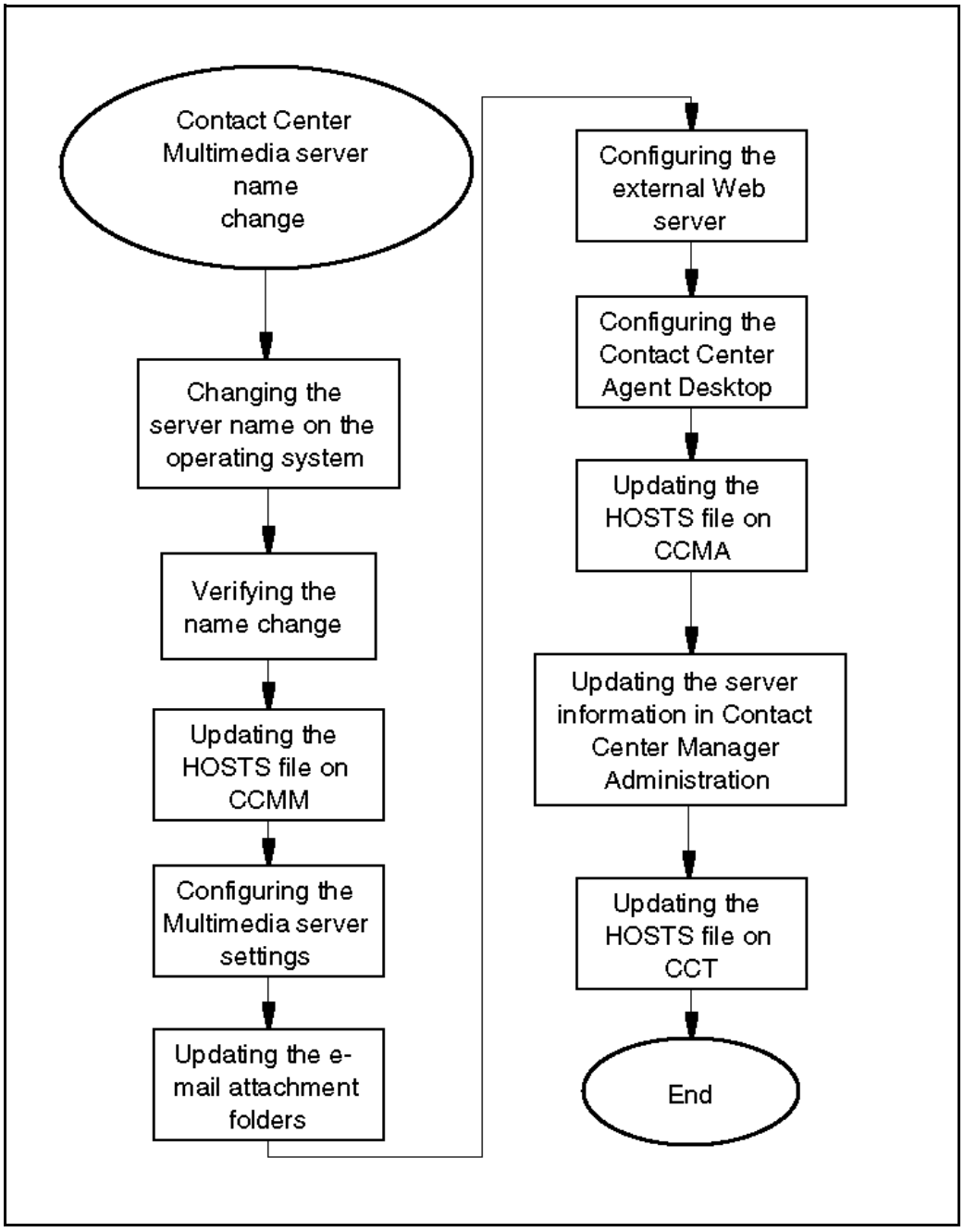
Prerequisites for CCMM server name change

- 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

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 (page 577).

CCMM server name change procedures



CCMM server name change navigation

- Changing the server name on the operating system (page 578)
- Verifying the server name change (page 578)
- Updating the HOSTS file (page 579) on CCMM
- Configuring the Multimedia server settings (page 580)

- Updating the e-mail attachment folders (page 581)
- Configuring the external Web server (page 582)
- Configuring the Agent Desktop (page 583)
- Updating the HOSTS file (page 579) on CCMA
- Updating the server information in Contact Center Manager Administration (page 583)
- Updating the HOSTS file (page 579) on CCT

Changing the server name on the operating system

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 steps

Step	Action
1	Log on to the Contact Center Multimedia server.
2	Choose **Start**, **Control Panel**, **System and Security**.
3	Under **System**, click **See the name of this computer**.
4	In the **Computer name, domain, and workgroup settings** section, click **Change settings**.
5	Click the **Computer Name** tab.
6	Click **Change**.
7	Enter the new server name.
8	Click **OK**.
9	Click **Yes** to restart the server.

--End--

Verifying the server name change

Verify that the Domain Name Service server or network has the correct server name.

Prerequisites

- Ensure that you use a Domain Name Service server in your network.

Procedure steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
server name	The new name of the server.

Updating the HOSTS file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer name to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: 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.

Procedure steps

Step	Action
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 of the Contact Center Multimedia server.
5	On the **File** menu, click **Save**.
6	Close all windows.

--End--

Configuring the Multimedia server settings

Configure the Contact Center Multimedia server name in the Multimedia Administrator application and ensure that the folders are labelled correctly to access the multimedia database.

Prerequisites

- Change the name of the Contact Center Multimedia server. See Changing the server name on the operating system (page 578).

Procedure steps

Step	Action
1	In the Contact Center Manager Administration application, click **Multimedia**.
2	Choose **General Administration**.
3	Click **Server Settings**.
4	On the Server Settings dialog box, select **Contact Center Multimedia Server**.
5	Click **Edit**.
6	In the **Server Name** box, type the name of the Contact Center Multimedia server.
7	In the **Server Port** box, change the port number of the server as required. The default server port is 1972.
8	To change the MCMC event port number, type the new number in the **MCMC Event Port** box. The default MCMC event port number is 7999.
9	Click **Save**.
10	A warning appears describing potential errors for changing this server. Click **OK** to accept.
11	Click **Close** to close the Server Settings dialog box.
12	On the Contact Center Multimedia server, navigate to the path D:\Avaya\Contact Center\Multimedia Server\Agent Desktop\CCADAppSettings.xml.
13	On the appropriate line of the text file, replace the name of the old Contact Center Multimedia server with the new Contact Center Multimedia server.
14	On the Contact Center Multimedia server, navigate to the path D:\Avaya\Contact Center\Multimedia Server\Outbound Client\OCMTappsetting.xml.
15	On the appropriate line of the text file, replace the name of the old Contact Center Multimedia server with the new Contact Center Multimedia server.
16	On the Contact Center Multimedia server, navigate to the path D:\Avaya\Contact Center\Multimedia Server\Common utilities\db.properties.
17	On the appropriate line of the text file, replace the name of the old Contact Center Multimedia server with the new Contact Center Multimedia server.

18	On the **Start** menu, click **Run**.
19	Type **scmu** to go to System Control and Monitor Utility.
20	Choose **CCMM** tab.
21	Click **Shutdown CCMM**.
22	Click **Start CCMM**.

--End--

Updating the e-mail attachment folders

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.

Prerequisites

- Ensure that you have the e-mail feature installed and enabled using the Contact Center License Manager.

Procedure steps

Step	Action
1	In the Multimedia Administrator, expand **Contact Center Multimedia**.
2	Expand **Email Administration**.
3	Double-click **Email Configuration**.
4	Click **Save**.
5	Close the Contact Center Multimedia Administrator.
6	On the **Start** menu, click **Run**.
7	Type **scmu** to go to System Control and Monitor Utility.
8	Choose **CCMM** tab.
9	Click **Shutdown CCMM**.
10	Click **Start CCMM**.

--End--

Configuring the external Web server

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.

Prerequisites

- Know the custom interface folder names and paths for the web.xml and .jsp files for the sample customer Web installation.

Procedure steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
CCMM_HOSTNAME	The name of the Contact Center Multimedia server.

Configuring the Agent Desktop

Configure the Agent Desktop to allow agents to monitor calls and make calls using the telephony toolbar.

Prerequisites

- 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 (page 578).

Procedure steps

Step	Action
1	Log on to the Agent desktop.
2	Change the URL that agents use to access the Agent Desktop to reflect the new server name.

--End--

Variable definitions

Variable	Value
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 server information in Contact Center Manager Administration

Update the Contact Center Multimedia server name in the Contact Center Manager Administration. 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.

Prerequisites

- Change the name of the Contact Center Multimedia server. Changing the server name on the operating system (page 578).

Procedure steps

Step	Action
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 **Add Server**.
5	On the Contact Center Manager Server **Properties** window, in the **Server Name** box, type the name of the Contact Center Multimedia server. *The system automatically completes the IP address and display name.*
6	In the **Login ID** box, type the logon ID for the reporting user name for the server.
7	In the **Password** box, type the password for the reporting user name for the server.
8	From the **Type** list, select **CCMM**.
9	Click **Submit**.
10	In the left pane, select the Contact Center Manager Server with which you want to associate the Contact Center Multimedia server.
11	Right-click the Contact Center Manager Server, and then click **Edit Properties**.
12	Under **Associated Reporting Server**, select the check box next to the current active Contact Center Multimedia server name.
13	Click **Submit**.
14	On the Launchpad menu, click **Logout**.

--End--

Variable definitions

Variables	Value
<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.

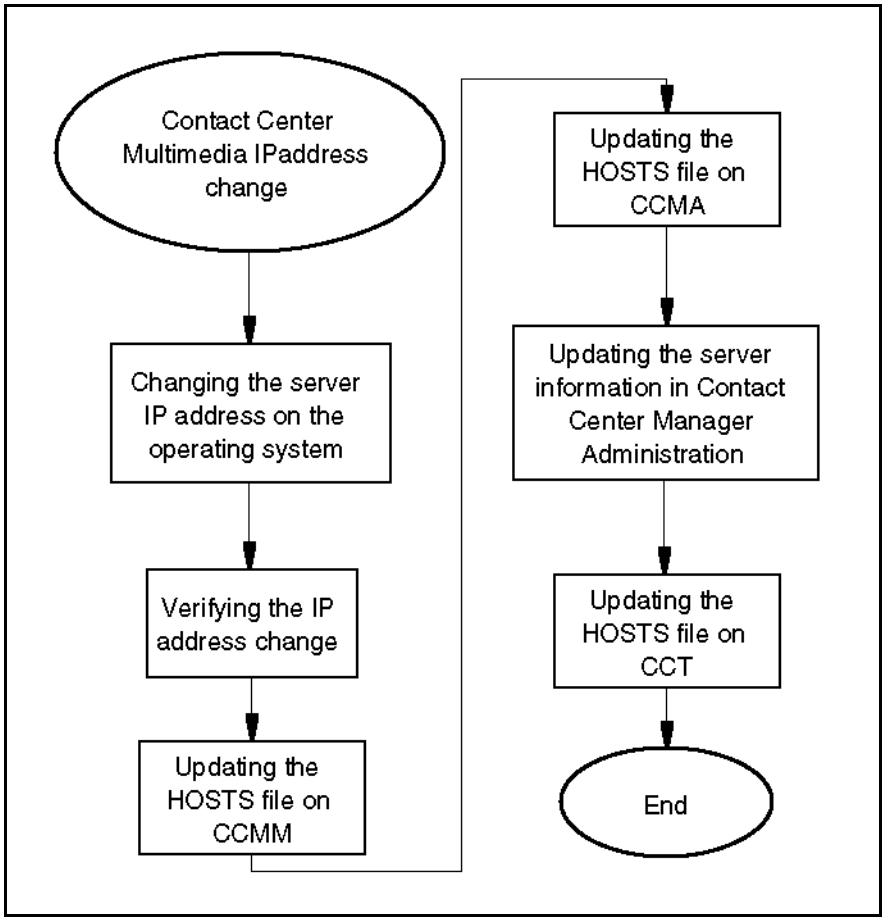
CCMM server IP address change

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

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 (page 585).

CCMM server IP address change procedures



CCMM server IP address change navigation

- Changing the IP address on the operating system (page 586)
- Verifying the server IP address change (page 586)
- Updating the HOSTS file (page 587) on CCMM
- Changing the IP address on the operating system (page 586)
- Updating the HOSTS file (page 587) on CCMA

- Updating the server information in Contact Center Manager Administration (page 588)
- Updating the HOSTS file (page 587) on CCT

Changing the IP address on the operating system

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.

Prerequisites

- Know how to stop and restart the Contact Center Multimedia services.

Procedure steps

Step	Action
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.

--End--

Verifying the server IP address change

Verify that the Domain Name Service server or network has the correct server IP address.

Procedure steps

Step	Action
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.

--End--

Variable definitions

Variable	Value
server name	The name of the Contact Center Multimedia server.

Updating the HOSTS file

If you have no DNS server, you must manually update the HOSTS file on each server in your contact center with the new computer IP address to ensure that all servers can interpret the new server name.

Prerequisites

- Determine if you need to update the HOSTS table on your server.

Attention: 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.

Procedure steps

Step **Action**

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 IP address of the Contact Center Multimedia server.

5 On the **File** menu, click **Save**.

6 Close all windows.

--End--

Updating the server information in Contact Center Manager Administration

Update the Contact Center Multimedia server name in the Contact Center Manager Administration. 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.

Prerequisites

- Change the name of the Contact Center Multimedia server. Changing the IP address on the operating system (page 586).

Procedure steps

Step	Action
1	Log on to the Contact Center Manager Administration server.
2	Log on to the Contact Center Manager Administration application as a user with administrative permissions.
3	Click **Configuration**.
4	From the **Server** menu, select **Add Server**.
5	On the Contact Center Manager Server **Properties** window, in the **Server Name** box, type the name of the Contact Center Multimedia server. *The system automatically completes the IP address and display name.*
6	In the **Login ID** box, type the logon ID for the reporting user name for the server.
7	In the **Password** box, type the password for the reporting user name for the server.
8	From the **Type** list, select **CCMM**.
9	Click **Submit**.
10	In the left pane, select the Contact Center Manager Server with which you want to associate the Contact Center Multimedia server.
11	Right-click the Contact Center Manager Server, and then click **Edit Properties**.
12	Under **Associated Reporting Server**, select the check box next to the current active Contact Center Multimedia server name.
13	Click **Submit**.
14	On the Launchpad menu, click **Logout**.

--End--

Variable definitions

Variables	Value
<CCMA_ServerName>	The name of the server where Contact Center Manager Administration is installed.

Variables	Value
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.

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.

Application	Default user ID	Default Password	Notes
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)	