Avaya Aura® Contact Center Commissioning

Release 6.2
NN44400-312
03.06
30 July 2012

© 2012 Avaya Inc.

All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

Copyright

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

Third-party components

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: New in this release 13
- Features 13
  - High Availability 13
  - LDAP server for voice contacts on Contact Center Multimedia server 15
  - Contact Center default certificates for Application Enablement Services (AES) 15
  - Avaya Media Server updates 15
  - Agent Greeting 16
  - Presence Services server for Instant Message contact types 16
- Other changes 17
  - SIP commissioning steps 17

Chapter 2: Introduction 19
- Prerequisites 19
- Related resources 19
  - Support 19
  - Avaya Mentor videos 20

Chapter 3: Avaya Aura® Contact Center server commissioning 21
- Prerequisites to Contact Center server commissioning 21
- Commissioning tasks for SIP-enabled Contact Center 21
- Commissioning tasks for AML-based Contact Center 27

Chapter 4: Contact Center Manager Server commissioning procedures 33
- Prerequisites for Contact Center Manager Server commissioning 33
- Contact Center Manager Server commissioning procedures 33
- Job aid: Timing 34
- Verifying the success of the installation 35
- Enabling Open Queue 35
- Enabling Multiplicity 36
- Configuring the operating system for remote access 37
- Disabling date and time features 38
- Disabling the Windows time service 38
- Verifying CCMS patches 39
- Scheduling weekly disk defragmentation 40
- Configuring the Multicast controller 40
- Confirming the CCMS services start 42

Chapter 5: Network Control Center commissioning 43
- Prerequisites for Network Control Center commissioning 43
- Network Control Center commissioning procedures 43
- Configuring the sites 44

Chapter 6: Avaya Media Server commissioning for non-HA deployments 47
- Prerequisites 48
- Avaya Media Server commissioning procedures 48
- Logging on to Avaya Media Server Element Manager 50
- Configuring the SIP port on a co-resident Avaya Media Server 51
- Configuring licensing on a standalone Avaya Media Server 51
- Configuring the primary Avaya Media Server for the cluster 52

Configuring a secondary Avaya Media Server for the cluster 53
Configuring a standard Avaya Media Server for the cluster 55
Adding the license file to the primary Avaya Media Server 56
Chapter 7: Avaya Media Server commissioning for HA deployments 57
Prerequisites 58
Avaya Media Server High Availability commissioning procedures 58
Logging on to Avaya Media Server Element Manager 60
Enabling High Availability on the primary Avaya Media Server 61
Obtaining the Universally Unique Identifier of the primary server 62
Configuring the High Availability pair primary Avaya Media Server 63
Enabling High Availability on the backup server 64
Configuring the High Availability pair backup Avaya Media Server 65
Adding the license file to the primary Avaya Media Server 67
Restarting the primary and backup servers 68
Configuring Content Store replication across multiple Avaya Media Server High Availability pairs 68
Configuring Content Store replication to an Avaya Media Server cluster at a remote site 70
Chapter 8: Avaya Media Server common commissioning 71
Configuring media on the Avaya Media Server 71
Prerequisites for Avaya Media Server common commissioning 73
Avaya Media Server common commissioning procedures 74
Logging on to Avaya Media Server Element Manager 76
Confirming the Contact Center packaged application locale 77
Silencing observation and barge-in tones 77
Configuring the Call Force Answer Zip Tone 78
Configuring a custom zip tone 79
Adding Contact Center Manager Server as a trusted node 81
Adding the media content namespace 81
Adding the locale-specific media content group 82
Uploading a batch zip file 83
Configuring continuous streamed source using RSS 85
Configuring continuous streamed source using SHOUTCast 86
Adding a media content group 87
Uploading a music media file 88
Uploading a treatment media file 89
Configuring Avaya Media Server settings for SIP-enabled contact center 91
Chapter 9: Avaya Media Server language commissioning 93
Prerequisites for Avaya Media Server language commissioning 96
Avaya Media Server language commissioning procedures 96
Configuring the contact center locale 98
Configuring contact center routes 99
Adding new media files 101
Updating the default media files 103
Creating a Contact Center flow application 105
Creating a Give Ringback Treatment block 107
Creating an Output block to play a greeting 108
Creating a Play and Collect IVR block 109
Creating a Play Prompt IVR block 112

Creating a Play Prompt IVR block to playback collected digits ... 113
Creating a call treatment block to play scripted music ... 115
Creating a Queue to Skillset block ... 116
Configuring the Flow Application Contact Router ... 117
Chapter 10: Contact Center Manager Administration commissioning ... 121
Prerequisites for Contact Center Manager Administration commissioning ... 121
Contact Center Manager Administration commissioning procedures ... 121
Job aid: Timing ... 125
Configuring the License Manager Service ... 126
Configuring Real-Time Reporting ... 127
Configuring domain accounts to allow scheduling Historical Reports to a Network Server ... 129
Creating a shared folder to export historical reports ... 129
Creating a shared folder on the client with read permissions for the domain ... 130
Creating a shared folder on the client with read permissions for a user ... 132
Creating a shared folder on the client PC with read permissions for the IUSR_SWC and CCMA Admin accounts ... 133
Configuring Agent Desktop Display parameters on the server ... 134
Downloading the latest documentation to the CCMA server ... 137
Creating a CCMA Certificate Signing Request ... 138
Installing the Signed Security Certificate Response ... 140
Installing the Root Security Certificate ... 141
Enabling HTTPS security for CCMA ... 142
Enabling communications with CCMA server components ... 143
Updating the CCMA Administration user password ... 144
Verifying the Web Services ... 145
Configuring Internet Explorer ... 145
Logging on to Contact Center Manager Administration for the first time ... 147
Adding the Contact Center Manager Server to Contact Center Manager Administration ... 149
Configuring Contact Center Manager Server Global Settings ... 150
Adding route points ... 151
Adding media servers ... 152
Adding media servers to the required services ... 154
Installing the Orchestration Designer client ... 155
Adding a Contact Center script or flow application ... 156
Chapter 11: Certificate Authority commissioning ... 159
Prerequisites to Certificate Authority commissioning ... 159
Certificate Authority commissioning procedures ... 160
Installing a standalone Certificate Authority ... 162
Exporting a Certificate Authority root certificate ... 164
Generating a signed certificate ... 165
Chapter 12: Contact Center Manager Server certificate commissioning ... 169
Prerequisites ... 170
Contact Center Manager Server certificate commissioning procedures ... 170
Removing the default certificates ... 172
Creating a certificate store using Certificate Manager ... 172
Generating a Certificate Signing Request file ... 175
Adding certificate files to the certificate store ... 178

Removing a certificate file from the certificate store ... 180
Examining a certificate file in the certificate store ... 182
Chapter 13: Security Framework commissioning ... 185
Prerequisites for Security Framework commissioning ... 185
Security Framework commissioning procedures ... 185
Job aid: Timing ... 186
Configuring workgroup server Fully Qualified Domain Name ... 187
Configuring the admin user for the Unified Communication Manager ... 188
Configuring the communication between CCMA and UCM ... 190
Creating Unified Communication Management local accounts ... 192
Mapping Unified Communication Management users to CCMA users ... 193
Starting Contact Center Manager Administration client ... 195
Configuring the admin user for the backup server ... 195
Configuring the communication between CCMA and the backup UCM ... 198
Chapter 14: Contact Center Manager Administration client commissioning ... 201
Prerequisites for client commissioning ... 201
Client commissioning procedures ... 201
Job aid: Timing ... 202
Configuring the display settings ... 203
Configuring Internet Explorer ... 203
Configuring display settings in Internet Explorer ... 205
Adding Internet Explorer to the firewall exceptions list ... 206
Opening multicast and unicast ports ... 206
Installing the ActiveX Controls ... 208
Applying the ActiveX Controls ... 209
Chapter 15: Communication Control Toolkit commissioning for SIP-enabled Contact Center ... 211
Prerequisites to CCT commissioning for SIP-enabled Contact Center ... 211
Communication Control Toolkit commissioning for SIP-enabled Contact Center procedures ... 212
Configuring the licensing for CCT ... 213
Configuring the deployment type for CCT ... 214
Confirming that the CCT services start ... 216
Adding the CCT Server in CCMA ... 216
Adding agents in CCMA for SIP-enabled Contact Centers ... 217
Verifying CCT using Reference Client ... 218
Chapter 16: Communication Control Toolkit commissioning for AML-based Contact Center ... 219
Prerequisites to CCT commissioning for AML-based Contact Center ... 219
Communication Control Toolkit commissioning for AML-based Contact Center procedures ... 220
Configuring the licensing for CCT ... 222
Configuring the deployment type for CCT ... 223
Confirming that the CCT services start ... 225
Adding the CCT Server in CCMA ... 225
Configuring the Avaya Communication Server 1000 service provider ... 226
Importing workstations from the domain ... 228
Importing Avaya Communication Server 1000 data ... 229
Adding an AML agent in CCMA ... 231

Assigning resources in Contact Center ... 232
Configuring Hotdesking (Agent Roaming) ... 234
Verifying CCT using the Reference Client ... 235
Chapter 17: Contact Center Multimedia server commissioning ... 237
Contact Center Multimedia server commissioning prerequisites ... 237
Contact Center Multimedia server commissioning procedures ... 238
Job aid: Timing ... 240
Providing local users with the Log on as a service right ... 240
Verifying the Multimedia database installation ... 241
Verifying that Contact Center Multimedia services start ... 241
Adding the multimedia servers to Contact Center Manager Administration ... 242
Logging on to the Multimedia Administration tool for the first time ... 244
Configuring server settings ... 245
Configuring an LDAP server for Agent Desktop voice contacts ... 247
Configuring the multimedia license type ... 248
Configuring e-mail recipient addresses ... 249
Configuring e-mail attachment file locations ... 251
Configuring the multimedia skillsets ... 253
Creating an Orchestration Designer application to route from an IM route point to an IM skillset ... 254
Configuring the MIME types ... 255
Chapter 18: Agent Desktop client commissioning ... 257
Prerequisites for Agent Desktop client commissioning ... 257
Agent Desktop client communications server commissioning procedures ... 257
Configuring hotdesking (optional) ... 259
Configuring the pop-up window for a Citrix environment ... 259
Chapter 19: Agent Greeting commissioning ... 261
Prerequisites for Agent Greeting commissioning ... 261
Agent Greeting commissioning procedures ... 261
Configuring Agent Greeting licensing on the Avaya Media Server ... 265
Configuring Agent Greeting on the Avaya Media Server ... 265
Configure a CDN to re-route calls to Agent Greeting ... 267
Adding SIP endpoints for the Avaya Media Server ... 269
Adding SIP Routing Entry for the Avaya Media Server ... 270
Creating a SIP Entity for Avaya Media Server ... 271
Creating a SIP Entity Link to the Avaya Media Server ... 274
Creating a routing policy from Session Manager to the Avaya Media Server ... 275
Creating a dial pattern to route calls to the Avaya Media Server ... 276
Adding the Avaya Media Server as a trusted host on the SES ... 277
Adding a routing entry for the Avaya Media Server ... 278
Adding a contact for the Agent Greeting dial pattern ... 278
Adding the Voice Proxy server as a trusted host on the Avaya MS ... 279
Enabling Agent Greeting on CCMS ... 280
Configuring Agent Greeting on CCMA ... 280
Enabling Agent Greeting in a voice-only Agent Desktop contact center ... 282
Enabling Agent Greeting for individual agents ... 283
Performing an end-to-end test ... 284
Chapter 20: Office Communications Server commissioning ... 285

Office Communications Server commissioning procedures ... 285
Ensuring that OCS supports TCP SIP Transport connection type ... 287
Adding Contact Center Manager Server as an authorized host ... 288
Adding a static route from OCS to Contact Center Manager Server ... 288
Chapter 21: Avaya Aura® Presence Services Instant Messaging application commissioning ... 291
Presence Services Instant Messaging chat server commissioning prerequisites ... 291
Presence Services Instant Messaging chat server commissioning procedures ... 292
Verifying the substitution rule to map the System Manager user login domain to the Presence Services domain ... 294
Creating a Presence Services user in System Manager for the route point ... 295
Adding an IM route point on CCMA for Presence Services ... 296
Creating a Presence Services user in System Manager for an agent ... 297
Adding the login ID to an agent's settings in CCMA ... 298
Creating a Presence Services user in System Manager for the IM web server ... 299
Creating an Orchestration Designer application to route from an IM route point to an IM skillset ... 301
Configuring the Instant Messaging chat server with the Presence Services server details ... 301
Running the Instant Messaging chat server ... 302
Sending an Instant Message to the contact center and verifying the routing to an agent ... 303
Chapter 22: Mission Critical High Availability campus co-resident server commissioning ... 305
Prerequisites ... 308
Mission Critical High Availability campus server commissioning procedures ... 309
Configuring Agent Desktop Standby CCT server ... 311
Resolving the Managed name to the Managed IP Address ... 312
Installing a third-party utility to support High Availability ... 313
Verifying services are ready for High Availability ... 313
Configuring High Availability on the Active Server ... 314
Configuring E-mail notification on the Active Server ... 317
Configuring service monitoring on the Active Server ... 319
Backing up the database on the Active Server ... 321
Restoring the database on the Standby Server ... 323
Configuring server details on the Standby Server ... 325
Configuring High Availability on the Standby Server ... 328
Starting the Active Server ... 331
Starting shadowing on the Standby Server ... 332
Verifying High Availability is running on the Active Server ... 333
Changing server details in Contact Center Manager Administration ... 334
Using the Contact Center Manager Administration server Managed name ... 335
Testing switchovers ... 336
Chapter 23: High Availability Remote Geographic Node server commissioning ... 337
Prerequisites ... 339
High Availability Remote Geographic Node server commissioning procedures ... 340
Installing a third-party utility to support High Availability ... 342
Verifying services are ready for High Availability ... 342
Configuring High Availability on the Active Server ... 343
Configuring E-mail notification on the Active Server ... 345
Configuring service monitoring on the Active Server ... 346

Backing up the database on the Active Server ... 348
Restoring the database on the Remote Geographic Node server ... 349
Configuring server details on the Remote Geographic Node server ... 351
Configuring High Availability on the Remote Geographic Node server ... 355
Starting the Active Server ... 356
Starting shadowing on the Remote Geographic Node Server ... 357
Verifying High Availability is running on the Active Server ... 358
Chapter 24: High Availability campus co-resident server commissioning ... 361
Prerequisites ... 364
High Availability Campus server commissioning procedures ... 365
Configuring Agent Desktop CCT server details ... 367
Resolving the Managed name to the Managed IP Address ... 368
Installing a third-party utility to support High Availability ... 369
Verifying services are ready for High Availability ... 369
Configuring High Availability on the Active Server ... 370
Configuring E-mail notification on the Active Server ... 373
Configuring service monitoring on the Active Server ... 374
Backing up the database on the Active Server ... 377
Restoring the database on the Standby Server ... 378
Configuring server details on the Standby Server ... 380
Configuring High Availability on the Standby Server ... 385
Starting the Active Server ... 387
Starting shadowing on the Standby Server ... 388
Verifying shadowing is running on the Active Server ... 390
Changing server details in Contact Center Manager Administration ... 392
Using the Contact Center Manager Administration server Managed name ... 393
Testing switchovers ... 394
Chapter 25: High Availability Geographic co-resident server commissioning ... 395
Prerequisites ... 397
High Availability Geographic co-resident server commissioning procedures ... 398
Installing a third-party utility to support High Availability ... 400
Verifying services are ready for High Availability ... 400
Configuring High Availability on the Active Server ... 401
Configuring E-mail notification on the Active Server ... 402
Configuring service monitoring on the Active Server ... 404
Backing up the database on the Active Server ... 406
Restoring the database on the Remote Geographic Node server ... 407
Configuring server details on the Remote Geographic Node server ... 409
Configuring High Availability on the Remote Geographic Node server ... 414
Starting the Active Server ... 415
Starting shadowing on the Remote Geographic Node server ... 416
Verifying shadowing is running on the Active Server ... 417
Chapter 26: High Availability campus CCMM commissioning ... 419
Prerequisites ... 421
High Availability CCMM commissioning procedures ... 421
Installing a third-party utility to support High Availability ... 423
Configuring CCMM General Administration ... 423

Configuring the Active Server ... 426
Backing-up the CCMM Active Server database ... 428
Restoring the database on the Standby Server ... 429
Configuring the Standby Server ... 430
Starting the Active Server ... 431
Starting shadowing on the Standby Server ... 431
Verifying shadowing is running on the Active Server ... 432
Testing a switchover on the CCMM solution ... 433
Chapter 27: Geographic High Availability CCMM commissioning ... 435
Prerequisites ... 435
Geographic High Availability CCMM commissioning procedures ... 436
Installing a third-party utility to support High Availability ... 438
Configuring CCMM General Administration ... 438
Configuring the Active Server ... 441
Backing-up the CCMM Active Server database ... 443
Restoring the database on the Remote Geographic Node server ... 444
Configuring RGN CCMM General Administration ... 445
Configuring the Remote Geographic Node Server ... 447
Starting the Active Server ... 448
Starting shadowing on the Remote Geographic Node Server ... 449
Verifying shadowing is running on the Active Server ... 449
Chapter 28: Communication Control Toolkit commissioning for Knowledge Worker. 451
Prerequisites to CCT commissioning for Knowledge Worker ... 451
Communication Control Toolkit commissioning for Knowledge Worker procedures ... 451
Confirming that the CCT services start ... 453
Configuring the licensing for CCT ... 454
Starting the CCT Web Administration application ... 455
Configuring the Avaya Communication Server 1000 service provider ... 456
Importing Avaya Communication Server 1000 Data ... 458
Importing Windows users from the CCT domain ... 461
Importing workstations from the domain ... 462
Assigning resources in Knowledge Worker ... 463
Configuring Hotdesking (Agent Roaming) ... 464
Verifying CCT using the Reference Client ... 465
Chapter 29: Integrated Reporting commissioning ... 467
Prerequisites for Integrated Reporting commissioning ... 467
Configuring licensing ... 470
Configuring Open Networking Web service ... 471
Configuring Integrated Reporting Server ... 472
Enabling Communication Control Toolkit Open Queue ... 474
Configuring landing pads ... 475
Enabling Contact Summary Reporting ... 477
Chapter 30: Contact Center Manager Server Web service configuration ... 479
Generating a Certificate Signing Request ... 479
Importing the CSR-Related Certificates ... 480
Configuring SOA OpenQueue and OpenNetworking Web Services ... 481
Removing Certificate Configuration ... 483

Chapter 31: Communication Control Toolkit Web service configuration **485**
Configuring SIP Call Recording **485**
Generating a Certificate Signing Request **486**
Importing CSR-related Certificates **487**
Configuring SOA CCT Web services **488**
Removing Certificate Configuration **490**
Chapter 32: Contact center testing **491**
Prerequisites **491**
Verifying correct operation **491**
Chapter 33: Common procedures **493**
Stopping individual services **493**
Starting services **493**
Disabling services **494**
Enabling services **494**
Stopping and restarting the core Communication Control Toolkit services **495**
Stopping and restarting the Contact Center Manager Server services **496**
Adding a server to a domain **496**
Starting the Contact Center **497**
Shutting down the Contact Center **498**
Index **499**

Chapter 1: New in this release

The following sections detail what is new in the *Avaya Aura® Contact Center Commissioning* (NN44400-312).

- Features on page 13
- Other changes on page 17

Features

See the following sections for information about feature changes:

- High Availability on page 13
- LDAP server for voice contacts on Contact Center Multimedia server on page 15
- Contact Center default certificates for Application Enablement Services (AES) on page 15
- Avaya Media Server updates on page 15
- Agent Greeting on page 16
- Presence Services server for Instant Message contact types on page 16

High Availability

Avaya Aura® Contact Center supports campus High Availability for fault tolerant and mission critical contact centers. Contact Center supports the following levels of campus High Availability:

- Mission Critical High Availability for SIP-enabled contact centers
- Hot-standby High Availability for AML-based contact centers
- Warm standby High Availability

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

Contact Center supports High Availability (HA) resiliency for Contact Center Manager Server (CCMS), Communication Control Toolkit (CCT), Contact Center Multimedia (CCMM), Avaya Media Server (MS) (Avaya MS), 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 of applications is called the active set. Another set of Contact Center applications in the same contact center system, runs in standby mode. This standby set of Contact Center applications monitors and shadows the active applications in the system but does not process calls. The standby CCMS monitors the active primary 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 active applications fails, the standby application recognizes the failure and starts processing contacts. You must configure the standby applications exactly the same as the active applications. Configuration changes to the active system during normal operation are automatically copied to the standby applications and the standby applications are configured to take over processing from the active system. Statistical data is also automatically copied to the standby applications.

Use the High Availability utility to configure High Availability for CCMS, CCT and CCMM. CCMA Active Directory Lightweight Directory Services (AD-LDS) replication is configured when installing CCMA.

Use the Contact Center System Management and Monitoring Component (SMMC) system tray for quick access to action items in your High Availability environment. Use SMMC to enable and start High Availability functionality.

For information about commissioning Mission Critical High Availability campus co-resident CCMS, CCMA and CCT, see Mission Critical High Availability campus co-resident server commissioning on page 305.

For information about commissioning hot-standby and warm standby High Availability campus co-resident CCMS, CCMA and CCT, see High Availability campus co-resident server commissioning on page 361.

For information about commissioning High Availability CCMM, see High Availability campus CCMM commissioning on page 419.

For information about commissioning geographic High Availability resiliency for a pair of co-resident CCMS and CCT servers in an Avaya Aura® Communication Manager and Avaya Aura® Session Manager Release 6.1 or 6.2 based solution, see High Availability Remote Geographic Node server commissioning on page 337.

For information about configuring geographic High Availability (HA) in an Avaya Communication Server 1000 based solution, see High Availability Geographic co-resident server commissioning on page 395.

For information about configuring geographic High Availability CCMM, see Geographic High Availability CCMM commissioning on page 435.

For information about commissioning Avaya Media Server (MS) High Availability, see Avaya Media Server commissioning for HA deployments on page 57.

LDAP server for voice contacts on Contact Center Multimedia server

Configuring a Lightweight Directory Access Protocol (LDAP) server provides agents with a list from which they can select contacts for making voice calls.

See Configuring an LDAP server for Agent Desktop voice contacts on page 247.

Contact Center default certificates for Application Enablement Services (AES)

Avaya Aura® Contact Center Release 6.2 supplies a set of default certificates for use with Application Enablement Services (AES). When you install Contact Center Manager Server it creates a certificate store containing the default certificates required to communicate with AES.

If you do not have access to or require a third-party Certificate Authority, you can install these Contact Center default certificates on your Application Enablement Services server to quickly setup a link between it and Avaya Aura® Contact Center.

Important:

AES 6.2 and later includes the default trust certificates. Using the default certificates Avaya Aura® Contact Center automatically communicates with AES.

For more information about Contact Center default security certificates, see CCMS certificate management on page 169.

Avaya Media Server updates

Avaya Aura® Contact Center supports a new deployment of Avaya Media Server (Avaya MS) to support the Contact Center High Availability (HA) feature. This deployment provides call protection for in-progress calls to the contact center. HA deployments of Avaya MS are supported only where Avaya MS is installed on the Linux operating system.

This book contains a re-organized chapter structure to separate and clarify the commissioning procedures for non-HA deployments, for HA deployments, and common to both deployments.

Non-HA deployments of Avaya MS have specific procedures for commissioning co-resident, single standalone, and multiple standalone Avaya MS servers. In a non-HA deployment, complete these procedures before implementing the Avaya MS common commissioning procedures. For more information about commissioning Avaya Media Server in a non-HA

contact center, see Avaya Media Server commissioning for non-HA deployments on page 47.

HA deployments of Avaya MS have specific procedures for commissioning single or multiple Avaya MS high-availability pairs. In a HA deployment, complete these procedures before implementing the Avaya MS common commissioning procedures. For more information about deploying Avaya Media Server for HA, see Avaya Media Server commissioning for HA deployments on page 57.

All Avaya MS deployments have common commissioning procedures. You must complete the deployment specific (non-HA or HA) procedures before implementing the Avaya MS common commissioning procedures. For more information about Avaya Media Server common procedures, see Avaya Media Server common commissioning on page 71.

Agent Greeting

The Agent Greeting feature allows agents to record personal greetings that the system can play automatically when an agent answers a voice contact. Agents can record time of the day greetings if the administrator configures the Time of Day settings. Only SIP-enabled Contact Centers support the Agent Greeting feature in Release 6.2; AML-based contact centers support Agent Greeting 3.0.

Application Module Link (AML) is an internal protocol used by Avaya Aura® Contact Center to communicate directly with the Avaya Communication Server 1000.

Agent Greeting has the following benefits:

- All callers receive a consistent greeting from the agent
- Agents have extra time to prepare for each call

For more information about Agent Greeting, see Agent Greeting commissioning on page 261.

Presence Services server for Instant Message contact types

Avaya Aura® Contact Center supports Avaya Aura® Presence Services as a chat server for Instant Message contact types. Using Avaya Aura® Presence Services as a chat server provides agents with improved presence information on Agent Desktop.

Avaya Aura® Presence Services integration is supported only on SIP-enabled contact centers based on the Avaya Aura® Release 6.1 and 6.2 platforms.

For more information about Presence Services support, see Avaya Aura® Presence Services Instant Messaging application commissioning on page 291.

Other changes

See the following sections for information about other changes in this document:

• SIP commissioning steps on page 17

SIP commissioning steps

New content related to commissioning your SIP-enabled Contact Center has been added to this document.

Chapter 2: Introduction

Avaya Aura® Contact Center Commissioning (NN44400-312) describes how to prepare the Avaya Aura® Contact Center Release 6.2 server and client software to handle inbound and outbound voice and multimedia contacts. Commissioning the server and client software prepares the hardware to run the contact center. If you want to make additional changes to the contact center server configuration, see the *Avaya Aura® Contact Center Server Administration* (NN44400-610).

Prerequisites

- Read the *Avaya Aura® Contact Center Overview* (NN44400-111).
- Read the *Avaya Aura® Contact Center Fundamentals* (NN44400-110).
- Read the *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Complete the *Avaya Aura® Contact Center Installation Checklist* (NN44400-310).
- Ensure that you understand the Contact Center features that you purchased.
- Install or migrate your Contact Center Release 6.2 software.
- Ensure that you know where each Contact Center component is installed.

Related resources

Support

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

Avaya Mentor videos

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

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

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

Chapter 3: Avaya Aura® Contact Center server commissioning

Commission the Contact Center software to prepare the features of the software for basic operation. This document contains separate workflows for commissioning both SIP-enabled and AML-based contact centers. To commission your SIP-enabled contact center, see Commissioning tasks for SIP-enabled Contact Center on page 21. To commission your AML-based contact center, see Commissioning tasks for AML-based Contact Center on page 27.

Prerequisites to Contact Center server commissioning

- Install or migrate your Contact Center software.

Commissioning tasks for SIP-enabled Contact Center

About this task

This work flow shows you the sequence of tasks you perform to commission the Contact Center software in your SIP-enabled contact center. To link to any task, go to SIP-enabled Contact Center commissioning navigation on page 26.

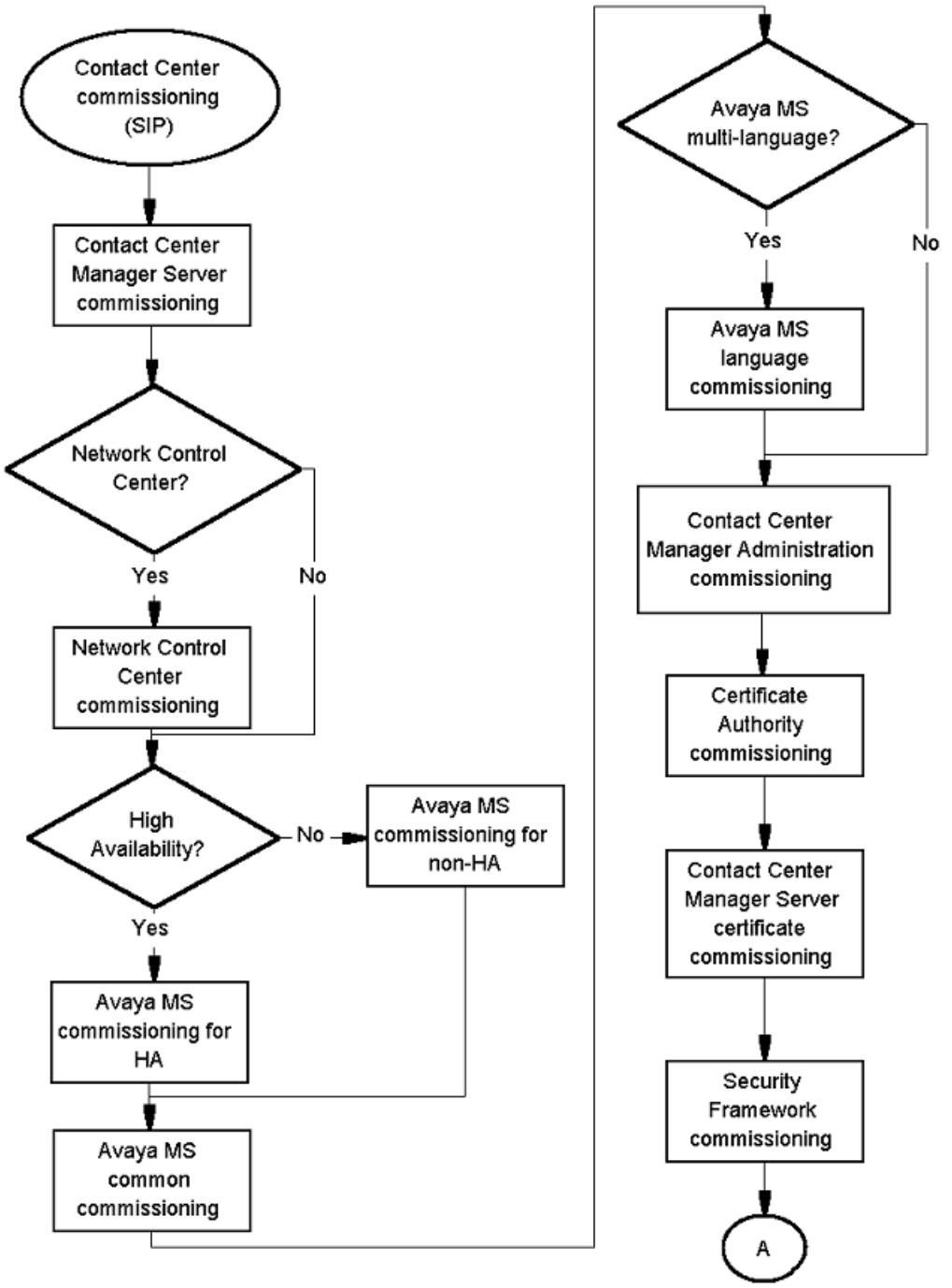


Figure 1: SIP-enabled Contact Center commissioning work flow

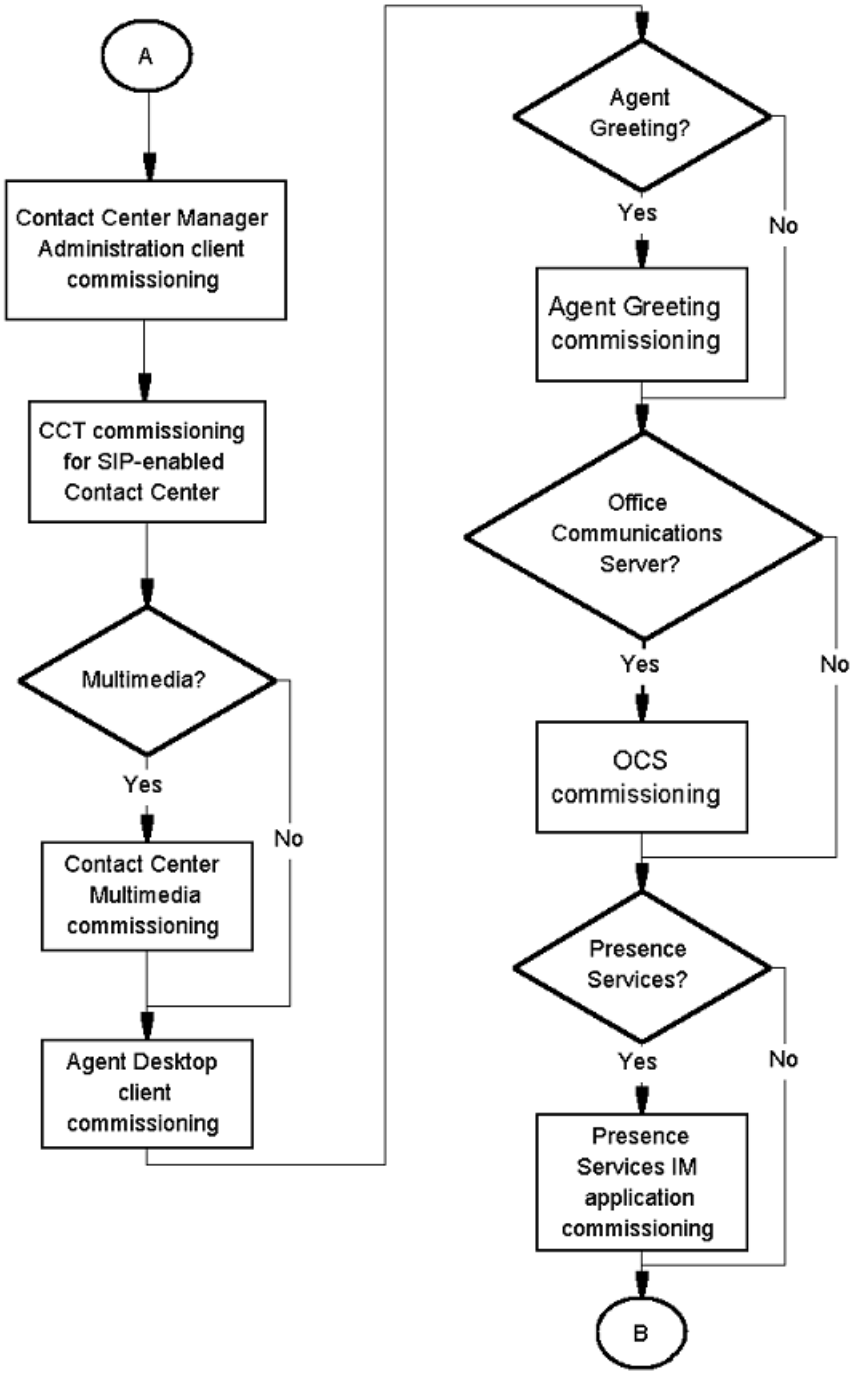


Figure 2: SIP-enabled Contact Center commissioning work flow continued

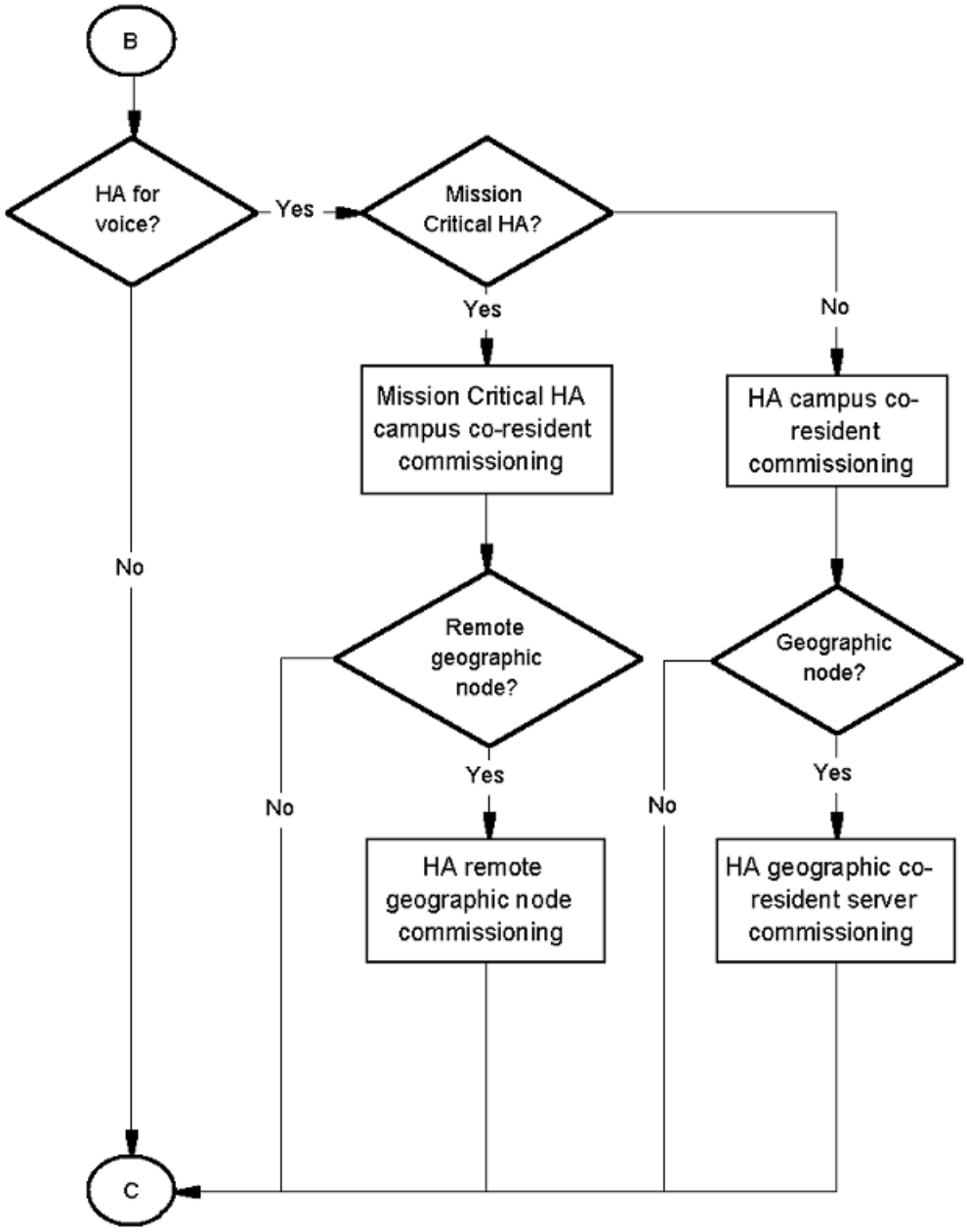


Figure 3: SIP-enabled Contact Center commissioning work flow continued

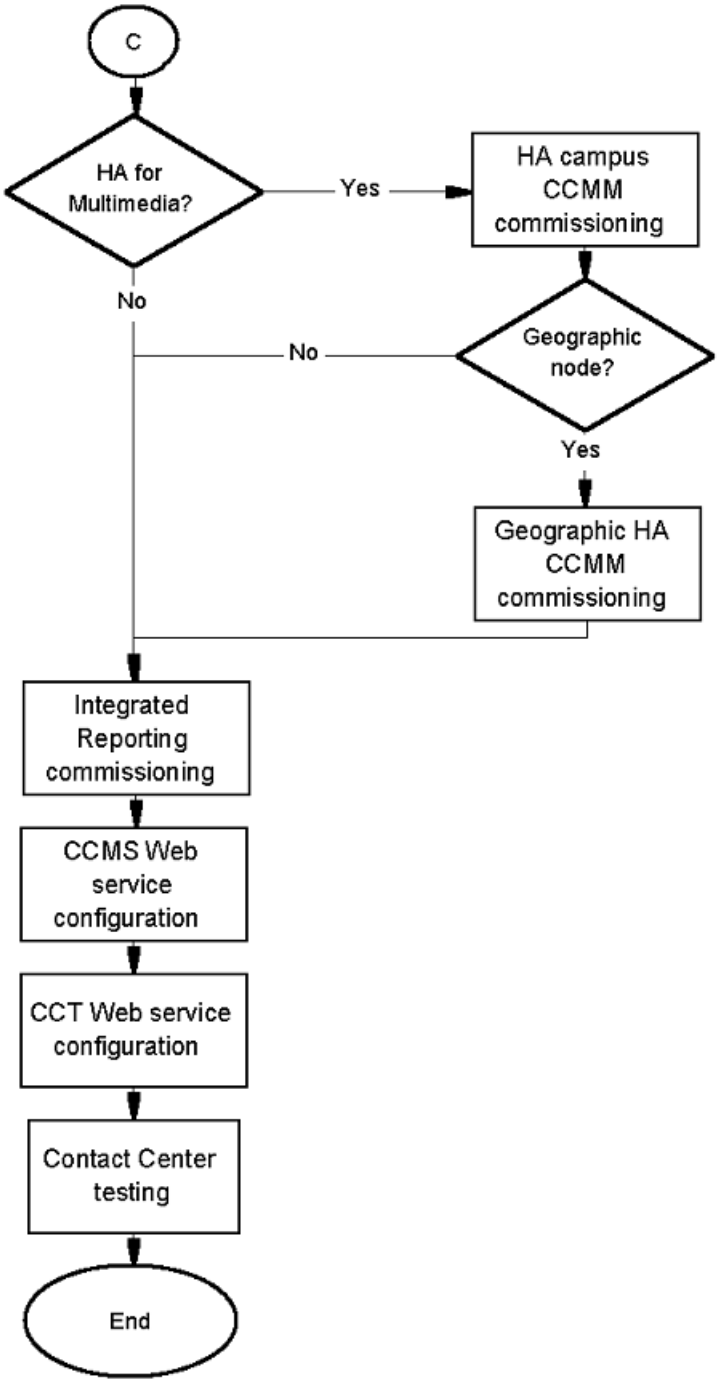


Figure 4: SIP-enabled Contact Center commissioning work flow continued

SIP-enabled Contact Center commissioning navigation

- Contact Center Manager Server commissioning on page 33
- Network Control Center commissioning on page 43
- Avaya Media Server commissioning for non-HA deployments on page 47
- Avaya Media Server commissioning for HA deployments on page 57
- Avaya Media Server common commissioning on page 71
- Avaya Media Server language commissioning on page 93
- Contact Center Manager Administration commissioning on page 121
- Certificate Authority commissioning on page 159
- Contact Center Manager Server certificate commissioning on page 169
- Security Framework commissioning on page 185
- Contact Center Manager Administration client commissioning on page 201
- Communication Control Toolkit commissioning for SIP-enabled Contact Center on page 211
- Contact Center Multimedia server commissioning on page 237
- Agent Desktop client commissioning on page 257
- Agent Greeting commissioning on page 261
- Office Communications Server commissioning on page 285
- Avaya Aura® Presence Services Instant Messaging application commissioning on page 291
- Mission Critical High Availability campus co-resident server commissioning on page 305
- High Availability Remote Geographic Node server commissioning on page 337
- High Availability campus co-resident server commissioning on page 361
- High Availability Geographic co-resident server commissioning on page 395
- High Availability campus CCMM commissioning on page 419
- Geographic High Availability CCMM commissioning on page 435
- Integrated Reporting commissioning on page 467
- Contact Center Manager Server Web service configuration on page 479
- Communication Control Toolkit Web service configuration on page 485
- Contact center testing on page 491

Commissioning tasks for AML-based Contact Center

About this task

This work flow shows you the sequence of tasks you perform to commission the Contact Center software in your AML-based contact center. To link to any task, go to AML-based Contact Center commissioning navigation on page 31.

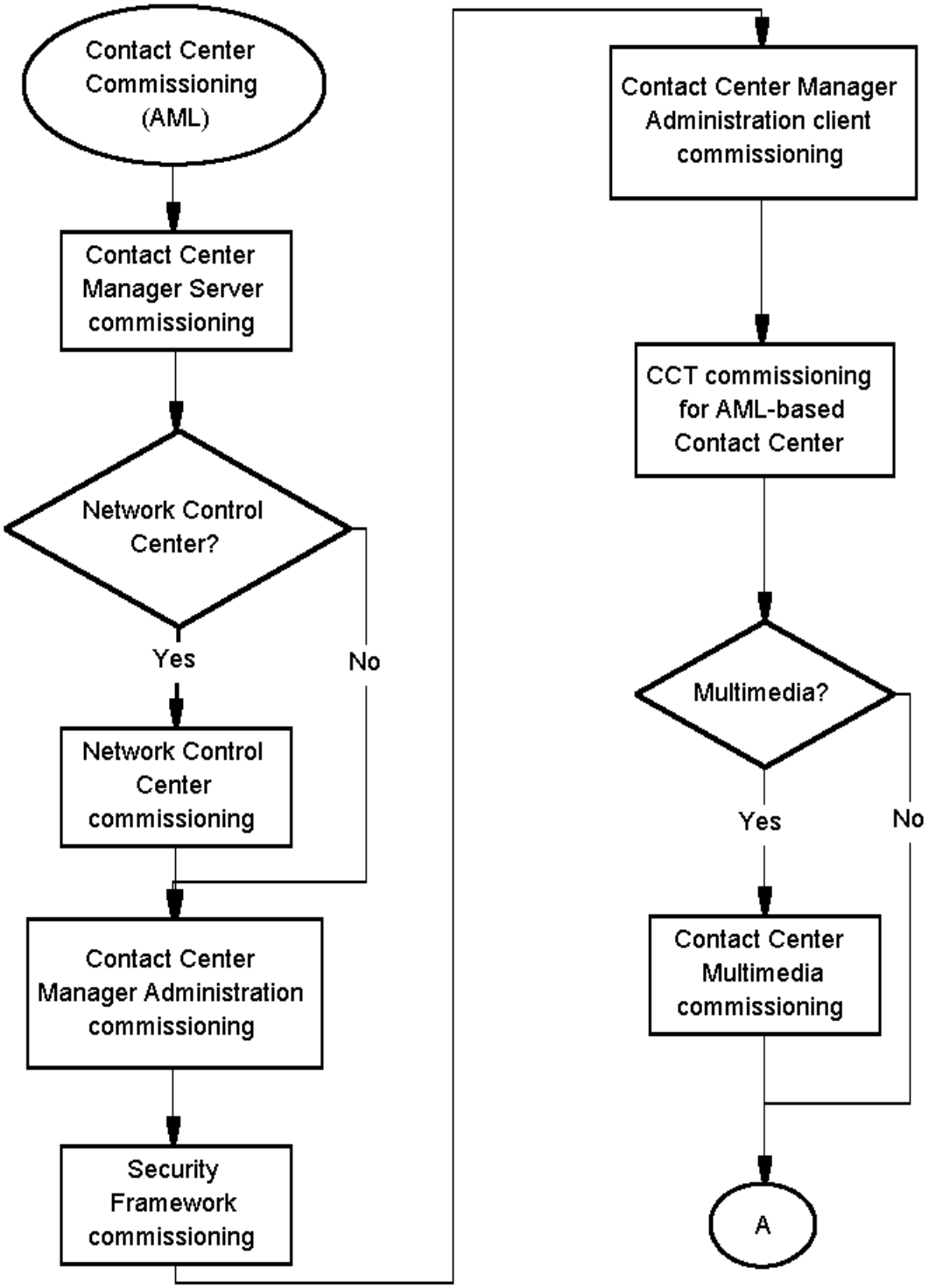


Figure 5: AML-based Contact Center commissioning work flow

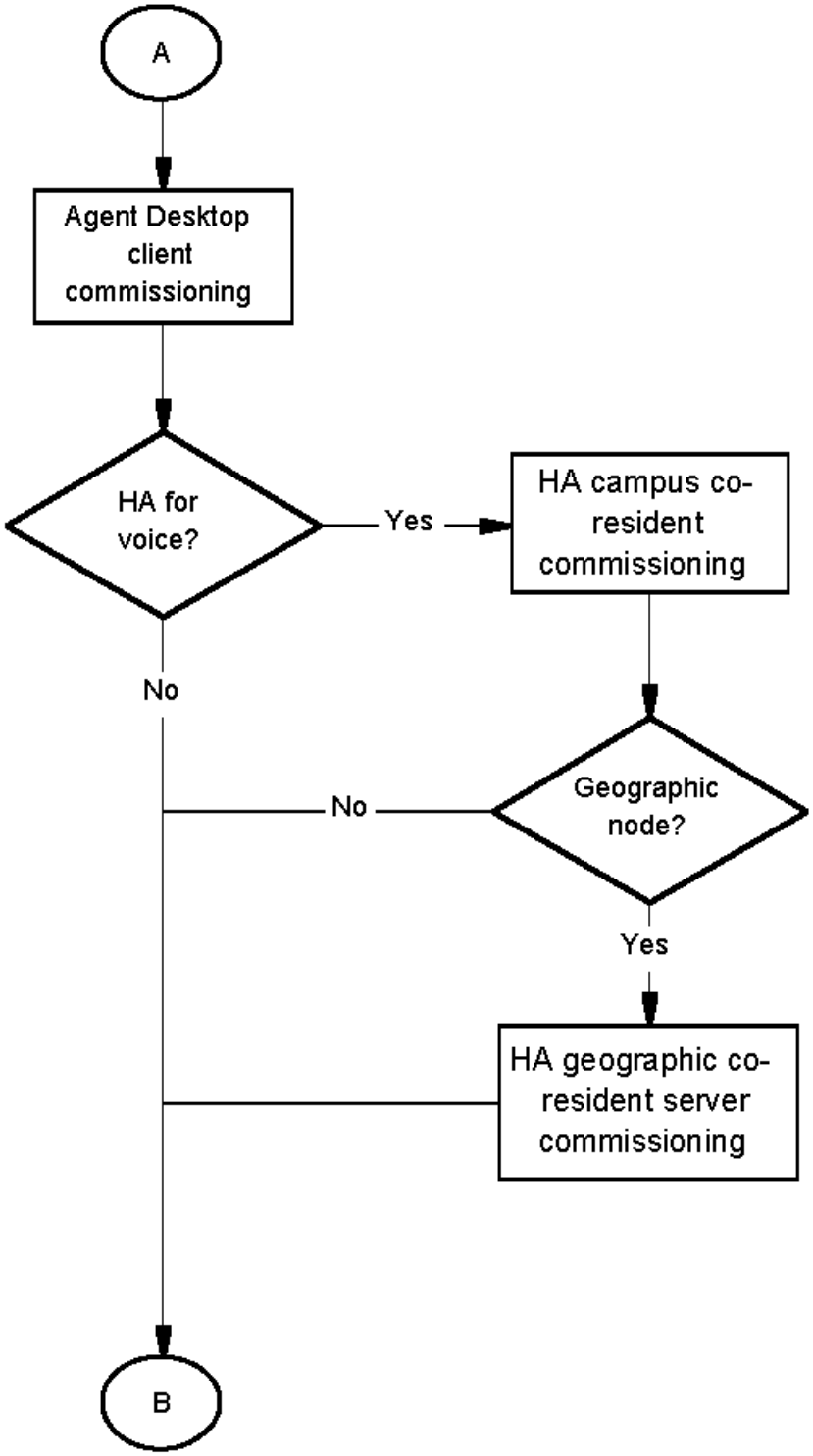


Figure 6: AML-based Contact Center commissioning work flow continued

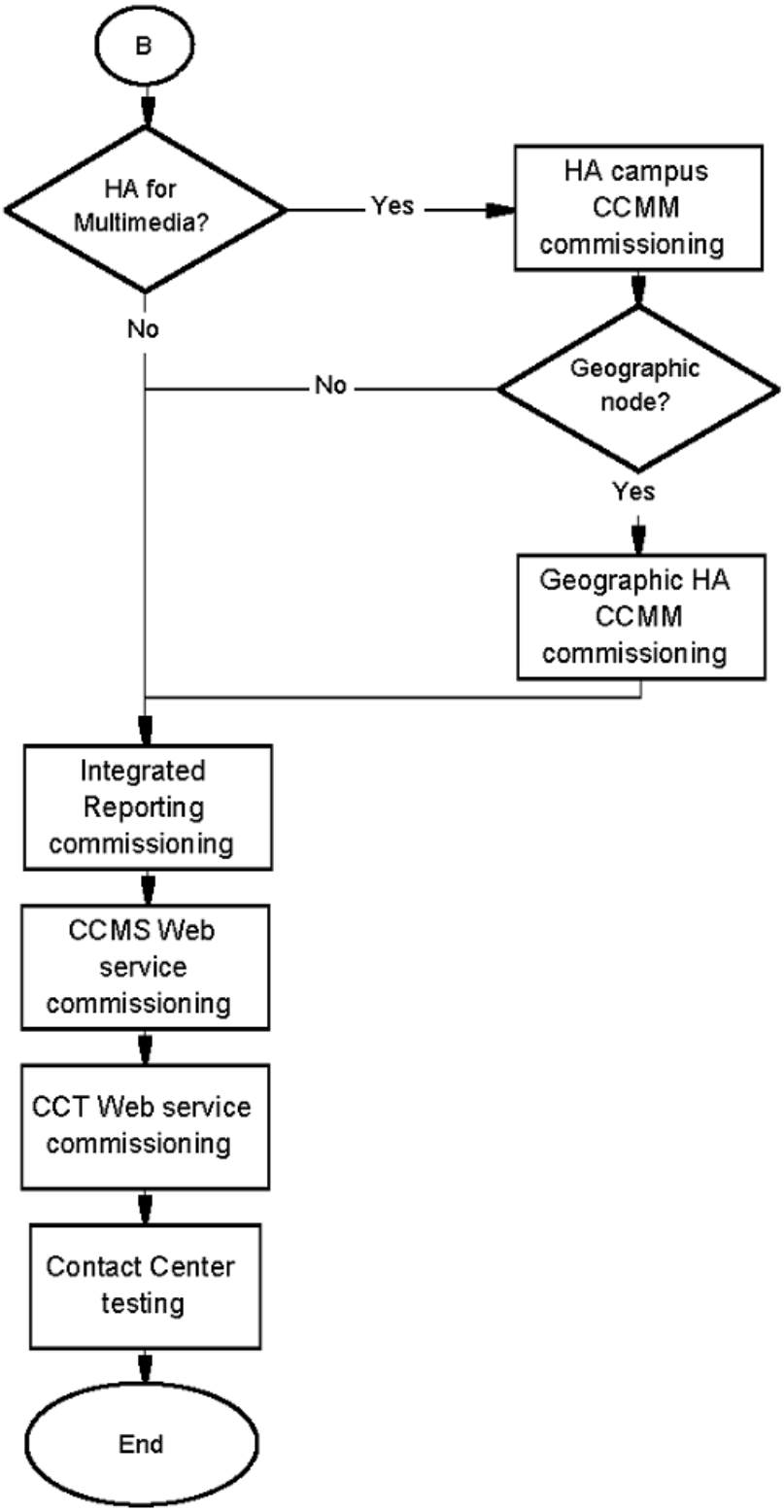


Figure 7: AML-based Contact Center commissioning work flow continued

AML-based Contact Center commissioning navigation

- Contact Center Manager Server commissioning on page 33
- Network Control Center commissioning on page 43
- Contact Center Manager Administration commissioning on page 121
- Security Framework commissioning on page 185
- Contact Center Manager Administration client commissioning on page 201
- Communication Control Toolkit commissioning for AML-based Contact Center on page 219
- Contact Center Multimedia server commissioning on page 237
- Agent Desktop client commissioning on page 257
- High Availability campus co-resident server commissioning on page 361
- High Availability Geographic co-resident server commissioning on page 395
- High Availability campus CCMM commissioning on page 419
- Geographic High Availability CCMM commissioning on page 435
- Integrated Reporting commissioning on page 467
- Contact Center Manager Server Web service configuration on page 479
- Communication Control Toolkit Web service configuration on page 485
- Contact center testing on page 491

Chapter 4: Contact Center Manager Server commissioning procedures

Use the procedures in this section to configure the Contact Center Manager Server software in your Avaya Aura® Contact Center. The procedures outlined include configuring your passwords, configuring features and verifying the success of your installation to prepare your server for Contact Center operations.

Prerequisites for Contact Center Manager Server commissioning

- Read the *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Complete the *Avaya Aura® Contact Center Installation Checklist* (NN44400-310).
- Read *Avaya Aura® Contact Center Installation* (NN44400-311).
- Install the Contact Center Manager Server software.
- Install the other Contact Center components on your server.

Contact Center Manager Server commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to configure Contact Center Manager Server.

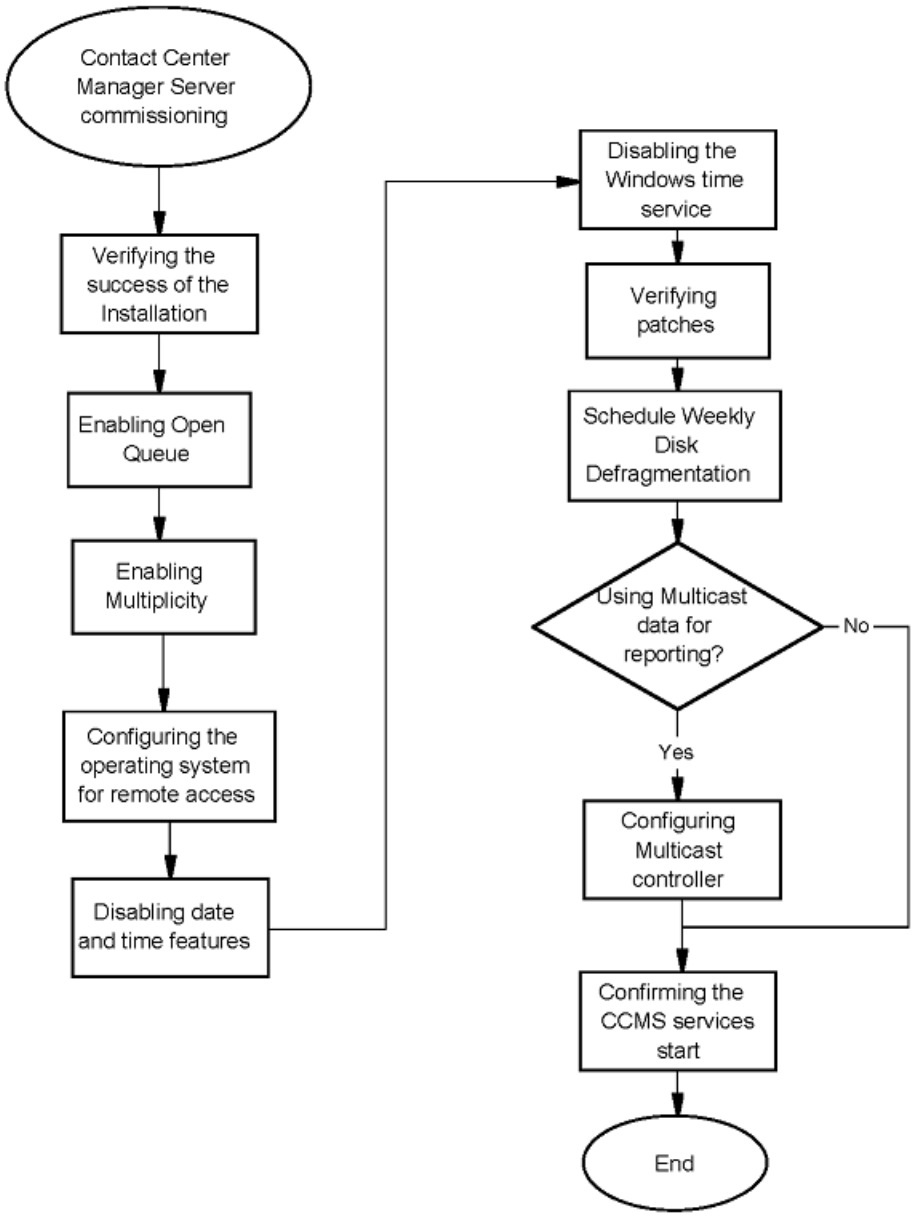


Figure 8: Contact Center Manager Server commissioning procedures

Job aid: Timing

The estimated time to commission Contact Center Manager Server is 1 hour.

Verifying the success of the installation

Before you begin

- Install the Contact Center Manager Server software.

About this task

Verify the success of your installation to ensure that all components are installed. To verify the success of the installation, ensure that the Contact Center Manager Server services are running.

Procedure

1. Log on to the server on which you installed Contact Center Manager Server as administrator.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**.
3. On the **CCMS** tab, check that all relevant services are in the **Up** state.
4. If you install a SIP-enabled Contact Center, verify that the SIP services started.
5. Close the System Control and Monitor Utility window.

Enabling Open Queue

Before you begin

- Install the Open Queue feature.
- Ensure that the Contact Center License Manager is licensed to provide Open Queue session licenses.
- Ensure that the Contact Center License Manager is licensed to provide agent licenses for the required contact types.

Important:

You must restart your server at the end of this procedure.

About this task

Enable Open Queue to allow third parties including Contact Center Manager Multimedia to create, read, and delete multimedia and voice contacts in Contact Center Manager Server.

Procedure

1. Log on to the server on which you installed Contact Center Manager Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
3. Click the **Licensing** tab.
4. From the **CCMS Optional Packages** list, select **Open Queue**.
5. Click **OK**.
6. Click **Yes** to restart the server.

Procedure job aid

After you restart Contact Center Manager Server, Open Queue is enabled. You must configure Controlled Directory Numbers (CDNs), also known as route points. The server uses these route points to route multimedia contacts. For more information, see the Contact Center Multimedia server commissioning on page 237.

Enabling Multiplicity

Before you begin

- Ensure that the Contact Center License Manager is licensed to provide Multiplicity.
- Ensure that the Contact Center License Manager is licensed to provide agent licenses for the required contact types.

Important:

You must restart your server at the end of this procedure.

About this task

Enable Multiplicity to allow agents manage multiple contact types at the one time. Configure multiplicity presentation classes (MPC) in CCMA. Each agent is assigned either the default MPC or a customized MPC. Enable multiplicity in the licensing tab of the Server Configuration utility.

Procedure

1. Log on to the server on which you installed Contact Center Manager Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.

3. Click the **Licensing** tab.
4. From the **CCMS Optional Packages** list, select **Multiplicity.**
5. Click **OK**.
6. Click **Yes** to restart the server.

Procedure job aid

After you restart Contact Center Manager Server, Multiplicity is enabled. Configure contact center agents for multiplicity in Contact Center Manager Administration using Multiplicity Presentation Classes. For more information, see the *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

Configuring the operating system for remote access

Before you begin

- If you use Contact Center Manager Server in a domain, add your Contact Center Manager Server to the domain before you configure remote access.

About this task

Configure remote access for your server to allow technical support to access the server.

Procedure

1. Log on to the server on which you installed Contact Center Manager Server.
2. Click **Start** > **Control Panel** > **System and Security** > **System**.
3. Click **Remote settings**.
4. In **System Properties**, select the **Remote** tab.
5. Under **Remote Desktop**, select **Allow connections from computers running any version of Remote Desktop (less secure)**.
6. Click **OK**.

Disabling date and time features

About this task

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

The contact center applications do not support time changes other than the Daylight Savings Change. Changing time causes issues with states of contacts.

If the Contact Center Manager Server is in a SIP environment, or is a Non Voice Multimedia installation, or is the Network Control Center server, skip this procedure.

Procedure

1. Click **Start** > **Control Panel**.
2. Under **Clock, Language, and Region**, click **Set the time and date**.
3. In the **Date and Time** dialog box, click **Change time zone**.
4. Clear the **Automatically adjust clock for daylight saving changes** check box.
5. Click **OK**.
6. Click the **Internet Time** tab.

   Important:

   If you click this tab and click OK without making changes, the Startup type for the Windows Time service is configured to Automatic.
7. Click **Change Settings**.
8. Clear the **Synchronize with an Internet time server** check box.
9. Click **OK**.
10. Click **OK** to close the dialog box.

Disabling the Windows time service

Before you begin

- Disable Date and Time features. See Disabling date and time features on page 38.

About this task

In an AML-based contact center, the CCMS server automatically synchronizes its time with the PABX. If the Windows Time service attempts to synchronize the CCMS server time with a

different time source, this can cause call processing outages. To avoid the potential for such problems, disable the Windows Time service.

If the Contact Center Manager Server is in a SIP environment, or is a Non Voice Multimedia installation, or is the Network Control Center server, skip this procedure.

Procedure

1. Click **Start** > **Administrative Tools** > **Services**.
2. In the Services window, in the right pane, double-click **Windows Time**.
3. In the **Windows Time Properties** dialog box, on the **General** tab, from the **Startup type** list, select **Disabled**.
4. Click **Stop**.
5. Click **Apply** to save your changes.
6. Click **OK** to close the **Windows Time Properties** dialog box.
7. Close the **Services** window.

Verifying CCMS patches

Before you begin

- Look up the most recent patches and upgrades for Contact Center Manager Server at www.avaya.com/support.
- Review *Avaya Aura® Contact Center Upgrade and Patches* (NN44400-410) to understand how to install patches and service packs.

About this task

Verify that you have the most recent patches for the Contact Center Manager Server software to ensure that your system runs the most up-to-date software.

Procedure

1. Log on to the server on which you installed Contact Center Manager Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **Contact Center Patch Manager**.
3. Click the **Contact Center Manager Server** tab.
4. View the **Update Name**.
5. Compare the 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 updates and patches from the Web site.

Scheduling weekly disk defragmentation

About this task

Schedule daily disk defragmentation for drive C and drive D to optimize performance and avoid potential outages.

Procedure

1. Click **Start** > **Computer**.
2. Right-click drive C and select **Properties**.
3. Click the **Tools** tab.
4. Select **Defragment Now**.
5. Click **Turn on Schedule**.
6. Select **Run on a schedule (recommended)**.
7. Under **Frequency**, select **Weekly**.
8. Under **Day**, select the day you want to schedule the defragmentation process.
9. Under **Time**, select an off-peak time at which you want to schedule the defragmentation process.
10. Click **Select Disks**.
11. In the **Disk Defragmenter: Select Disks for Schedule** window, select drive C and drive D.
12. Click **OK**.
13. Click **OK**.
14. Click **Close**.

Configuring the Multicast controller

About this task

Configure the Multicast controller if you plan 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. For Unicast delivery, only one user can log on at a time and you must ensure that you disconnect all terminal services sessions.

For more information about multicast and unicast, see *Avaya Aura® Contact Center Fundamentals* (NN44400-110).

Procedure

1. Log on to the server on which you installed Contact Center Manager Server as administrator.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Multicast Stream Control**.
3. In the **RTD Multicast Controller** dialog box, select the check boxes for the Real Time data to enable.
4. In the **Compression** section of the window, select the **RTD Compression** check box.
5. Clear the **RSM Compression** check box.
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 for Contact Center Manager Server to use 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 for the number of network hops packets can transition

    OR

    Type a new value.

    Important:

    Do not change the ports.
11. For the **Interval to Date**, **Moving Window IP Port**, and **Multicast Rate** boxes, accept the default values.
12. Click **Apply**.
13. Click **OK**.
14. Click **Start** > **All Programs** > **Administrative Tools** > **Services**.
15. Scroll down to **CCMS SDP_Service**.

16. Click **Restart**.

Confirming the CCMS services start

About this task

Confirm that all appropriate Contact Center Manager Server services start on the Contact Center Manager Server.

Use the System Control and Monitor Utility to start and stop all applications in Contact Center including the license manager. The System Control and Monitor Utility can also start, stop, or monitor the services in Contact Center Manager Server.

Procedure

1. Log on to the Contact Center Manager Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**.
3. Click the **Contact Center** tab.
4. Select the applications to start on the current server by selecting the application name check boxes.
5. Click **Start Contact Center**.
6. Click the **CCMS** tab.
7. Ensure that all services in the **Profile** box have a green circle next to them.
8. If some of the services do not start, click **Start CCMS**.
9. Click **Close**.

Chapter 5: Network Control Center commissioning

Configure the communications database to enable the distribution of information from the Network Control Center (NCC) database to all servers on the network and to enable communication and network skill-based routing (NSBR) among multiple sites. The communications database lists all servers in the network, including each IP addresses and status.

Prerequisites for Network Control Center commissioning

- Install the Network Control Center server software.
- Install a Contact Center Manager Server at each site.
- Install and commission the Contact Center License Manager software.
- Install and commission Contact Center Manager Administration.
- If you use an Avaya Communication Server 1000, configure the following elements:
  - NACD (not required for Universal Networking)
  - a CDN for the server to use as an MCDN Network CDN (not required for Universal Networking)
  - Landing Pads (required for Universal Networking only)
  - a dialing plan to facilitate call routing between the telephony switches
- If you use a Microsoft Office Communications Server (with a Communication Server 1000 PABX for voice calls), configure a dialing plan to facilitate call routing between the telephony switches (on the Avaya Communication Server 1000).
- Ensure that all site names and the CLAN IP addresses are unique.

Network Control Center commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to commission the Network Control Center to use for the first time.

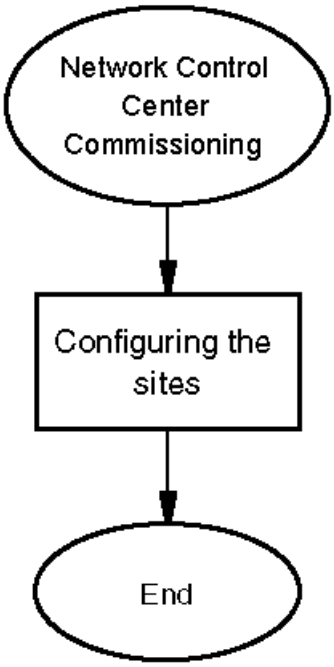


Figure 9: Network Control Center commissioning navigation

Configuring the sites

About this task

Configure the sites on the networked Avaya Aura® Contact Center on the Network Control Center server to designate the site names and locations.

Procedure

1. On the Network Control Center server, choose **Start** > **Run**.
2. In the **Open** box, type **nbconfig –admin**.
3. Click **OK**.
4. Click the **Site Table** tab.

Important:

Do not select the Force Synchronization check box. When you force synchronization, you force each site in the network to request address table information from every other site in the network. This can result in unnecessary use of network bandwidth. (Normally, servers request address table updates only

when the NCC notifies them that the site list changed.) Use the Force Synchronization option if information at a site is not updated.

5. Click **Add**.
6. In the **CLAN IP Address** box, enter the CLAN IP address of the server.

   Important:

   Each server must have a unique CLAN IP address.

7. Click **OK**.
8. Repeat step 5 on page 45 to step 7 on page 45 for each server on your network.
9. After you add the servers, click **Verify** to validate the connection to the nodal servers.
10. If all site names are correct, click **Apply** to update the database and synchronize the site table.

    The Flags column shows the progress of synchronization.

11. Click **Refresh** to update the status of the flags. Synchronization is complete when an N appears in the Flags column beside the NCC, and an S appears beside each server.
12. Click the **Address Table** tab.

    The communication addresses of the new servers appear on the Address Table page.

Chapter 6: Avaya Media Server commissioning for non-HA deployments

Use the procedures in this chapter to commission Avaya Media Server (Avaya MS) only if your contact center does not implement the High Availability (HA) feature. If the contact center implements the High Availability feature, see Avaya Media Server commissioning for HA deployments on page 57.

Avaya Media Server (Avaya MS), a software based media processing server, provides Avaya Aura® Contact Center with conferencing, announcements, dialogs, and the Agent Greeting feature.

Avaya Media Server is supported only in SIP-enabled contact centers.

In a non-High Availability deployment of Avaya Media Server, the following configurations are possible:

- Avaya Media Server installed co-resident with other contact center components on a Windows Server 2008 Release 2 64-bit operating system.

  When installed co-resident with Contact Center Manager Server, Avaya Media Server uses the Contact Center License Manager and the license server on Avaya Media Server is disabled.

- A single standalone Avaya Media Server on a Windows Server 2008 Release 2 64-bit operating system.

  When installed on a standalone server, Avaya Media Server uses the Avaya Media Server License Server and the Contact Center Services for Avaya Media Server licenses must be applied using the Avaya Media Server Element Manager.

- A single standalone Avaya Media Server on a Red Hat Enterprise Linux 5.x 32-bit operating system. Avaya Media Server is supported only when Red Hat Linux is installed with English Language selected.

  When installed on a standalone server, Avaya Media Server uses the Avaya Media Server License Server and the Contact Center Services for Avaya Media Server licenses must be applied using the Avaya Media Server Element Manager.

- Multiple Avaya Media Servers on a Windows Server 2008 Release 2 64-bit operating system.

  To configure more than 1000 agents on a SIP contact center, deploy multiple Avaya Media Servers in a cluster configuration. You must still configure each Avaya Media Server separately in CCMA.

When using a Windows-based Avaya Media Server cluster, the Avaya Media Server License Server and the Contact Center Services for Avaya Media Server licenses must be installed on the primary Avaya Media Server Element Manager.

- Multiple Avaya Media Servers, each installed on a server with the Red Hat Enterprise Linux 5.x 32-bit operating system. Avaya Media Server is supported only when Red Hat Linux is installed with English Language selected.

  To configure more than 1000 agents on a SIP contact center, deploy multiple Avaya Media Servers in a cluster configuration. You must still configure each Avaya Media Server separately in CCMA.

  When using a Linux based Avaya Media Server cluster, the Avaya Media Server License Server and the Contact Center Services for Avaya Media Server licenses must be installed only on the Avaya Media Server Element Manager.

The servers in an Avaya Media Server cluster must all have the same operating system. All the servers in an Avaya Media Server cluster must use the Windows Server 2008 Release 2 64-bit operating system, or all the servers must use the Red Hat Enterprise Linux 5.x 32-bit operating system. Avaya Media Server does not support clusters with mixed operating systems.

WebLM licensing

When using WebLM licensing, do not configure WebLM licensing on Avaya Media Server. When you configure an Avaya Media Server as a Media Server in Contact Center Manager Administration, Contact Center License Manager pushes the license keys to that Avaya Media Server. You must restart that Avaya Media Server so it can acquire these licenses and operate in Nodal Licensing mode.

Prerequisites

- You have read the Avaya Media Server chapter in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- You have installed Avaya Media Server software.

Avaya Media Server commissioning procedures

About this task

This task flow shows the sequence of procedures to commission Avaya Media Server in a contact center that does not implement High Availability.

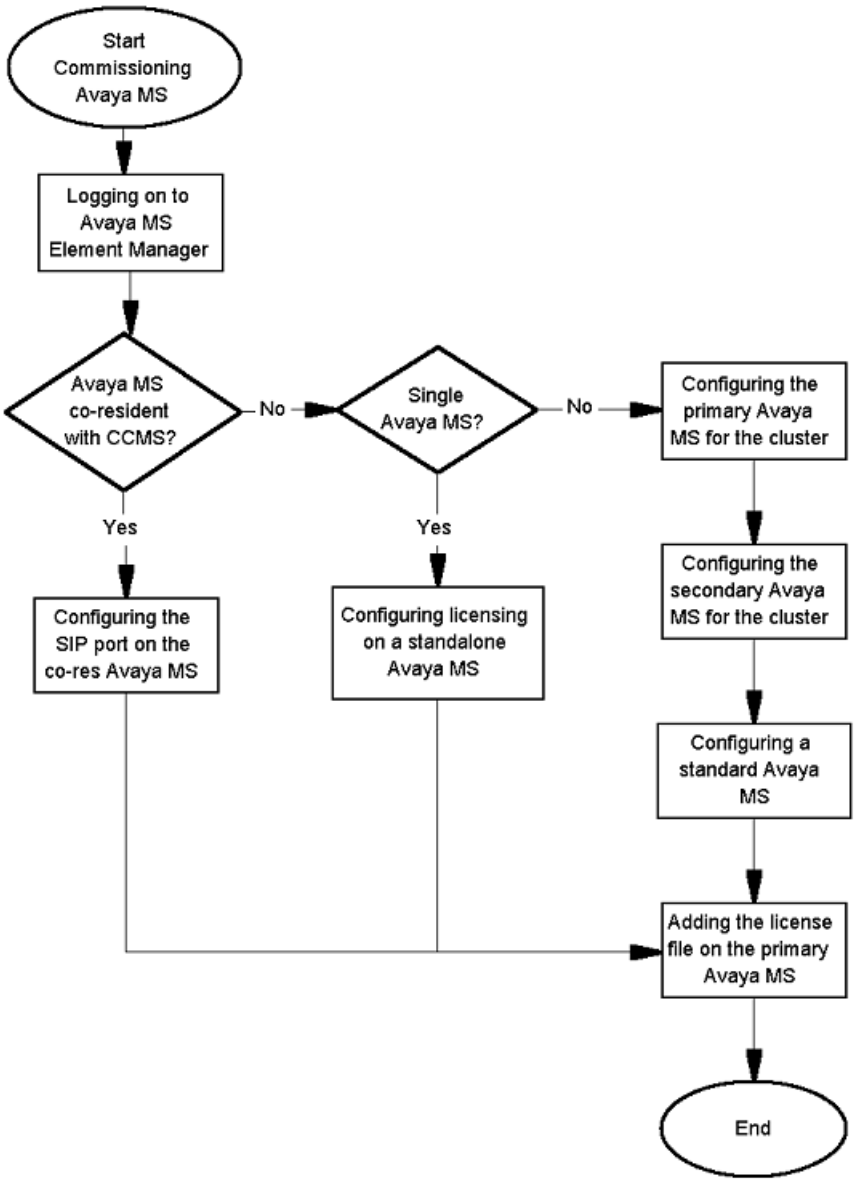


Figure 10: Avaya Media Server commissioning procedures taskflow

Logging on to Avaya Media Server Element Manager

Before you begin

- Obtain a valid user name and password to access Avaya Media Server Element Manager.

About this task

Log on to the Avaya Media Server Element Manager as an administrator to configure Avaya Media Server.

Element Manager (EM) is a web-based administration tool that facilitates the Operation, Administration, and Maintenance (OAM) of Avaya Media Server. A SIP-enabled Contact Center solution must contain one or more Avaya Media Server servers. Each Avaya Media Server server in the Contact Center solution must be licensed and configured to provide media services.

Procedure

1. On the Avaya Media Server server, start a Web browser.
2. In the address box, enter https://SERVER_IP_ADDRESS:8443/em. Where SERVER_IP_ADDRESS is the IP address of the Avaya Media Server.
3. In the **User ID** box, type the Avaya Media Server User ID log on account name. The default Element Manager User ID account name is the Avaya MS server administrator account name. If Avaya Media Server is installed on a Windows server, the default administrator account name is *Administrator*. If Avaya Media Server is installed on a Linux server, the default administrator account name is *root*.
4. In the **Password** box, type the Avaya Media Server Element Manager password. The default Element Manager password is the administrator password for the Avaya MS server.
5. Click **Log in**.

Related topics:

Procedure job aid on page 76

Comments? infodev@avaya.com

Configuring the SIP port on a co-resident Avaya Media Server

Before you begin

- Access the Element Manager for the Avaya Media Server.

About this task

If Avaya Media Serveris installed co-resident with Contact Center Manager Server, configure the Avaya Media Server SIP port so that it does not have a port clash with the Contact Center Manager Server SIP port. On a standalone Avaya Media Server server, the default Avaya Media Server SIP port number is 5060.

Procedure

1. In the navigation pane, click **System Configuration**.
2. Click **Network Settings**.
3. Click **Advanced Settings**.
4. In the **sipudp** box in the **MAS SIP UserAgent** component, type **5070**.
5. Click **Save**.

Configuring licensing on a standalone Avaya Media Server

Before you begin

- Access the Element Manager for the Avaya Media Server.

About this task

Add the license file to the Avaya Media Server and set it as a license server.

Note:
If you are using WebLM licensing, skip this procedure.

Procedure

1. In the navigation pane, click **Licensing**.
2. Click **General Settings**.

3. Select License Server from the **Licensing** list.
4. In the **Replace License Keys** box, paste the license key for this server.
5. Click **Validate**.
   Avaya MS validates the key and displays the licenses in the license details list.
6. Click **Save**.

Configuring the primary Avaya Media Server for the cluster

About this task

Designate an Avaya Media Server as the primary server for a cluster, and create a replication username and password.

Procedure

1. Log on to the Element Manager for the primary Avaya Media Server.
2. In the navigation pane, click **Cluster Configuration**.
3. Select **Server Designation**.
4. Under **Local Servers**, select **Primary** from the **Role** list.
5. Under **Replication Account**, select the **Enable Replication Account** check box.
6. In the **Username** box, type a username for the replication account. This value is arbitrary, but you must use the same value for all servers in the cluster.
7. In the **Password** box, type a password for the replication account. This value is arbitrary, but you must use the same value same value for all servers in the cluster.
8. Click **Save**.
9. Under **Local Servers**, note the **UUID** value. You must enter this value on the other servers in the cluster.

Procedure job aid

Configure an Avaya Media Server as a primary server so that other servers in the cluster can replicate configuration from it.

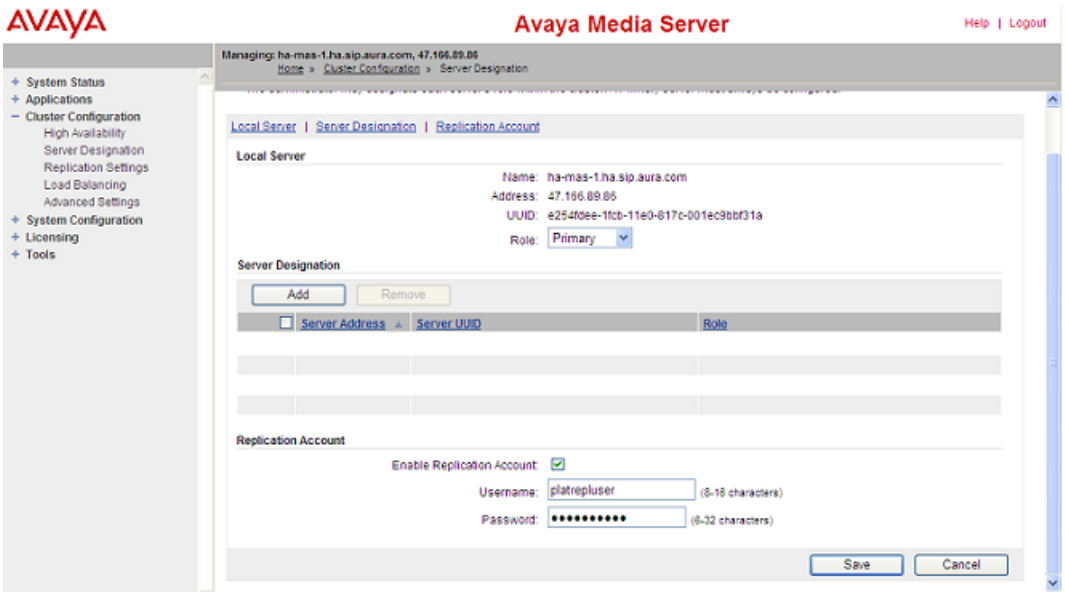


Figure 11: Example of configuring an Avaya Media Server as a primary server

Configuring a secondary Avaya Media Server for the cluster

Before you begin

- Designate an Avaya Media Server as the primary server for a cluster, and create a replication username and password.

About this task

Designate a secondary Avaya Media Server for the cluster. Configure the secondary server with the primary Avaya Media Server UUID and IP address, and enter the replication account details.

Procedure

1. Access the Element Manager for the secondary Avaya Media Server.
2. In the navigation pane, click **Cluster Configuration**.
3. Select **Server Designation**.

4. Under **Local Servers**, select Secondary from the **Role** list.
5. Under **Server Designation**, type the UUID of the Primary server in the **Primary Server UUID** box.
6. Type the primary server IP address in the **Primary Server Address** box.
7. Under **Replication Account**, select the **Enable Replication Account** check box.
8. In the **Username** box, type the username for the replication account that you specified on the primary server.
9. In the **Password** box, type the password for the replication account that you specified on the primary server.
10. Click **Save**.

Procedure job aid

Configure the secondary Avaya Media Server to enter the primary server UUID and IP address, and the replication account for the cluster.

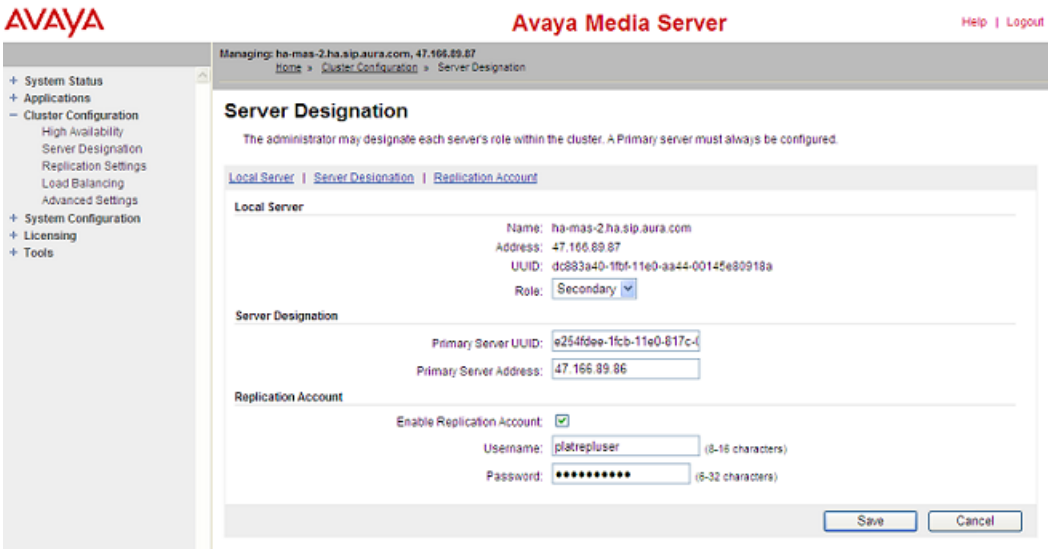


Figure 12: Example of designating an Avaya Media Server as a secondary server

Configuring a standard Avaya Media Server for the cluster

Before you begin

- Designate an Avaya Media Server as the primary server for a cluster, and create a replication username and password.
- Designate a secondary Avaya Media Server for the cluster.

About this task

Designate any remaining Avaya MS servers as standard servers for the cluster. Configure each standard Avaya Media Server with the primary Avaya Media Server UUID and IP address, and enter the replication account details.

Procedure

1. Access the Element Manager for the standard Avaya Media Server.
2. In the navigation pane, click **Cluster Configuration**.
3. Select **Server Designation**.
4. Under **Local Servers**, select Standard from the **Role** list.
5. Under **Server Designation**, type the UUID of the Primary server in the **Primary Server UUID** box.
6. Type the primary server IP address in the **Primary Server Address** box.
7. Under **Replication Account**, select the **Enable Replication Account** check box.
8. In the **Username** box, type the username for the replication account that you specified on the primary server.
9. In the **Password** box, type the password for the replication account that you specified on the primary server.
10. Click **Save**.

Adding the license file to the primary Avaya Media Server

Before you begin

- Obtain an Avaya Media Server license key from Avaya.

About this task

Add the license file to the primary Avaya Media Server and designate this server as a license server. The other servers (secondary and standard) in the cluster get their licensing from this primary server.

In an Avaya Media Server cluster, the license key must contain the MAC addresses of both the primary and the secondary servers.

Note:

If you are using WebLM licensing, skip this procedure.

Procedure

1. Log on to the Element Manager for the primary Avaya Media Server.
2. In the navigation pane, click **Licensing**.
3. Click **General Settings**.
4. Select License Server from the **Licensing** list.
5. In the **Replace License Keys** box, paste the license key for this cluster.
6. Click **Validate**.
   The Avaya Media Server validates the key and displays the licenses in the license details list. The list shows each license type twice, one entry for each MAC address.
7. Click **Save**.

Comments? infodev@avaya.com

Chapter 7: Avaya Media Server commissioning for HA deployments

Use the procedures in this chapter to commission Avaya Media Server (Avaya MS) only if your contact center implements the High Availability (HA) feature. If the contact center does not implement the High Availability feature, see Avaya Media Server commissioning for non-HA deployments on page 47.

The Avaya Media Server High Availability feature ensures uninterrupted availability of media processing and reduces loss of processing data when an Avaya Media Server fails. This provides call protection to the contact center.

The High Availability feature uses two media servers operating in a stand-by deployment. Both the servers have identical configuration and provide full media processing capabilities.

Administrators configure the High Availability feature by designating one server as the primary server and the other as the backup server. Both servers communicate with each other using a heartbeat mechanism.

Interruptions in the heartbeat from the primary server trigger a failover to the backup server. As both the primary and backup servers are identical in functionality and configuration, the failover is seamless to Contact Center.

The following considerations apply to Avaya Media Servers using High Availability:

- High Availability can be configured only in a 1+1 configuration (a high availability pair).
- High Availability is available only if the Avaya Media Servers are installed on the Red Hat Enterprise Linux 5.x 32-bit operating system.
- Once the backup server becomes active there is no automatic fallback to the primary server.

To restore the primary server the administrator must manually set the backup server status to “Failover”.

One Avaya Media Server high availability pair supports up to 1000 agents. To configure more than 1000 agents on a HA SIP contact center, deploy multiple Avaya Media Servers high availability pairs, and configure replication from the primary of one of the HA pairs.

You must still configure each Avaya Media Server Content Store replication pair separately in Contact Center Manager Administration.

WebLM licensing

When using WebLM licensing, do not configure WebLM licensing on Avaya Media Server. When you configure an Avaya Media Server as a Media Server in Contact Center Manager Administration, Contact

Center License Manager pushes the license keys to that Avaya Media Server. You must restart that Avaya Media Server so it can acquire these licenses and operate in Nodal Licensing mode.

Prerequisites

- Read the Avaya Media Server chapter in *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Install two Avaya Media Servers on the Red Hat Enterprise Linux 5.x 32-bit operating system. Avaya Media Server is supported only when Red Hat Linux is installed with English Language selected.
- Choose one server for use as the primary server and the other for use as the backup server.
- Select a managed IP address for the high availability pair. You must configure the managed IP address on both the primary and the backup servers. During a failover the backup server starts accepting all calls received on this IP address.
- Ensure both servers can ping their own Fully Qualified Domain Name (FQDN) and the other server FQDN, either by modifying the servers' hosts files or by entering appropriate entries on the network DNS server.

Important:

This task flow requires restarting both Avaya Media Servers.

Avaya Media Server High Availability commissioning procedures

About this task

This task flow shows the sequence of procedures to commission High Availability on one or more pairs of Avaya Media Servers.

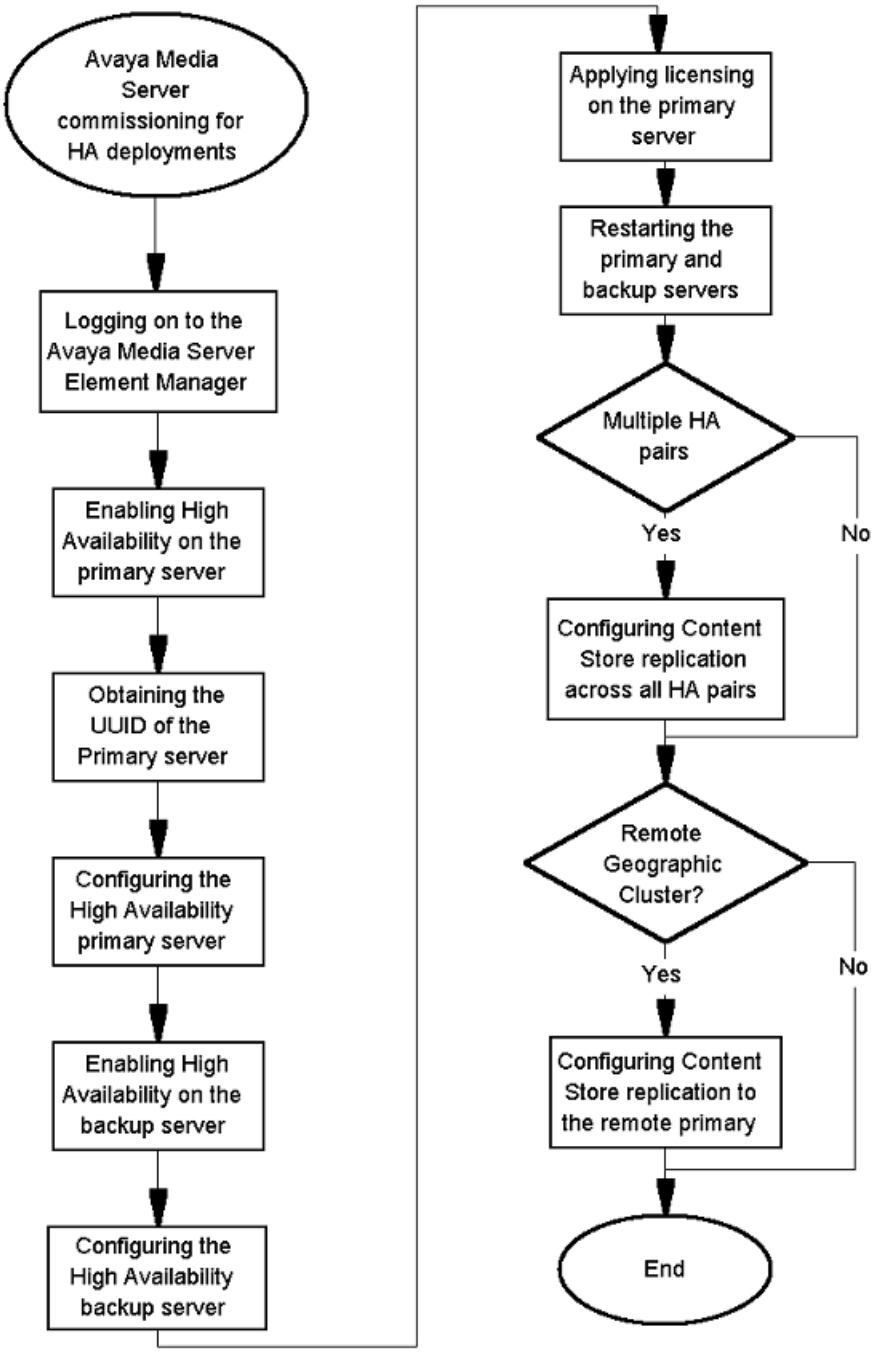


Figure 13: Avaya Media Server High Availability commissioning procedures

Logging on to Avaya Media Server Element Manager

Before you begin

- Obtain a valid user name and password to access Avaya Media Server Element Manager.

About this task

Log on to the Avaya Media Server Element Manager as an administrator to configure Avaya Media Server.

Element Manager (EM) is a web-based administration tool that facilitates the Operation, Administration, and Maintenance (OAM) of Avaya Media Server. A SIP-enabled Contact Center solution must contain one or more Avaya Media Server servers. Each Avaya Media Server server in the Contact Center solution must be licensed and configured to provide media services.

Procedure

1. On the Avaya Media Server server, start a Web browser.
2. In the address box, enter https://SERVER_IP_ADDRESS:8443/em. Where SERVER_IP_ADDRESS is the IP address of the Avaya Media Server.
3. In the **User ID** box, type the Avaya Media Server User ID log on account name. The default Element Manager User ID account name is the Avaya MS server administrator account name. If Avaya Media Server is installed on a Windows server, the default administrator account name is *Administrator*. If Avaya Media Server is installed on a Linux server, the default administrator account name is *root*.
4. In the **Password** box, type the Avaya Media Server Element Manager password. The default Element Manager password is the administrator password for the Avaya MS server.
5. Click **Log in**.

Related topics:

Procedure job aid on page 76

Comments? infodev@avaya.com

Enabling High Availability on the primary Avaya Media Server

Before you begin

- Select one Avaya Media Server as the primary server.
- Access the Element Manager for the primary Avaya Media Server.

About this task

Enable High Availability on the primary Avaya Media Server. Configure Avaya Media Server to notify Contact Center Manager Server when an Avaya Media Server failure or switchover occurs.

If you have more than one Avaya Media Server High Availability pair, select one server from each Avaya Media Server pair to be the primary Avaya Media Server server. Perform this procedure on the primary Avaya Media Server of each High Availability pair.

Procedure

1. In the primary Avaya Media Server Element Manager navigation pane, click **Cluster Configuration**.
2. Click **High Availability**.
3. Under **General Settings**, select the **Enable High Availability** check box.
4. In the **Service IP Address** box, type the managed IP address for this Avaya Media Server High Availability pair.
5. In the **Service IP Address Mask** box, type the subnet mask for the managed IP address.
6. Under the Failure Notification List, click **Add** to add the Contact Center Manager Server managed IP address.
   Avaya Media Server sends a notification to Contact Center Manager Server if a failover occurs.
7. In the **Server Address** box, type the managed IP address of the Contact Center Manager Server server.
8. In the **Server Port** box, type **57012**. This Avaya Media Server - **Failure Notification List** - **Server Port** number must match the Contact Center Manager Server High Availability utility - **Local SMMC Port** number.
9. Click **Save**.

Procedure job aid

Configure an Avaya Media Server primary server to start creating a High Availability pair.

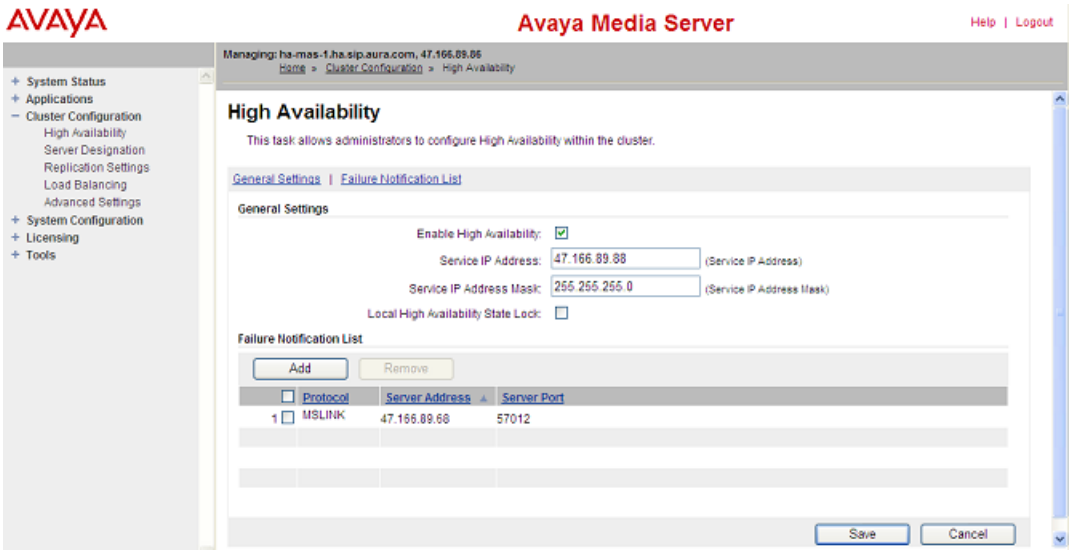


Figure 14: Example of configuring Avaya Media Server High Availability on the primary server

Obtaining the Universally Unique Identifier of the primary server

Before you begin

- Access the Element Manager for the primary Avaya Media Server.

About this task

Perform this procedure to obtain the Universally Unique Identifier (UUID) of the primary Avaya Media Server. You need to enter the primary server UUID when you configure the backup server in the high availability pair.

If you have more than one Avaya Media Server High Availability pair, select one server from each Avaya Media Server pair to be the primary Avaya Media Server server. Perform this procedure on the primary Avaya Media Server of each High Availability pair.

Procedure

1. In the primary Avaya Media Server Element Manager navigation pane, click **System Status**.
2. Click **Element Status**.

3. Record the UUID for the primary Avaya Media Server from the Element Status page.

Configuring the High Availability pair primary Avaya Media Server

Before you begin

- Access the Element Manager for the primary Avaya Media Server.

About this task

Designate the primary Avaya Media Server as the primary server in each High Availability pair, and create a replication username and password for the high availability pair.

If you have more than one Avaya Media Server High Availability pair, select one server from each Avaya Media Server pair to be the primary Avaya Media Server server. Perform this procedure on the primary Avaya Media Server of each High Availability pair.

Procedure

1. In the navigation pane, click **Cluster Configuration**.
2. Click **Server Designation**.
3. Under **Local Servers**, from the **Role** list, select **Primary**.
4. Under **Replication Account**, select the **Enable Replication Account** check box.
5. In the **Username** box, type a username for the replication account. This value is arbitrary, but you must use the same value on the backup server.
6. In the **Password** box, type a password for the replication account. This value is arbitrary, but you must use the same value on the backup server.
7. Click **Save**.

Procedure job aid

Configure the primary Avaya Media Server to create a replication account for the High Availability pair.

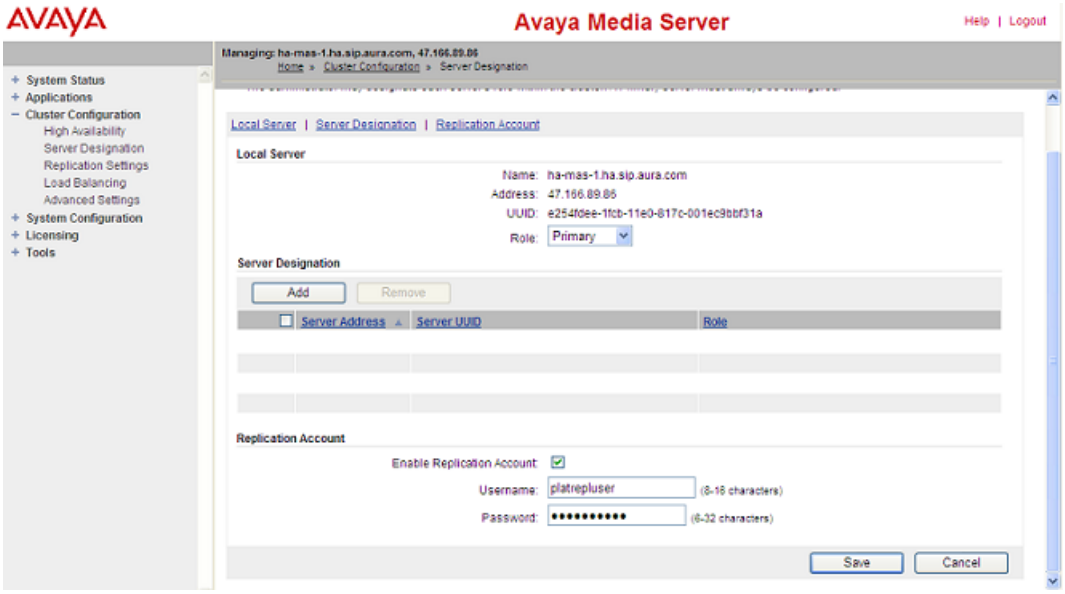


Figure 15: Example of designating an Avaya Media Server as a primary server

Enabling High Availability on the backup server

Before you begin

- Access the Element Manager for the backup Avaya Media Server.

About this task

Configure the backup server to start replicating from the primary server for High Availability.

If you have more than one Avaya Media Server High Availability pair, select one server from each Avaya Media Server pair to be the backup Avaya Media Server server. Perform this procedure on the backup Avaya Media Server of each High Availability pair.

Procedure

1. In the backup Avaya Media Server Element Manager navigation pane, click **Cluster Configuration**.
2. Click **High Availability**.
3. Under **General Settings**, select the **Enable High Availability** check box.
4. In the **Service IP Address** box, type the managed IP address for this High Availability pair.
5. In the **Service IP Address Mask** box, type the subnet mask for the managed IP address.

6. Click **Save**.

Procedure job aid

Enable High Availability on an Avaya Media Server backup server to complete creating a High Availability pair.

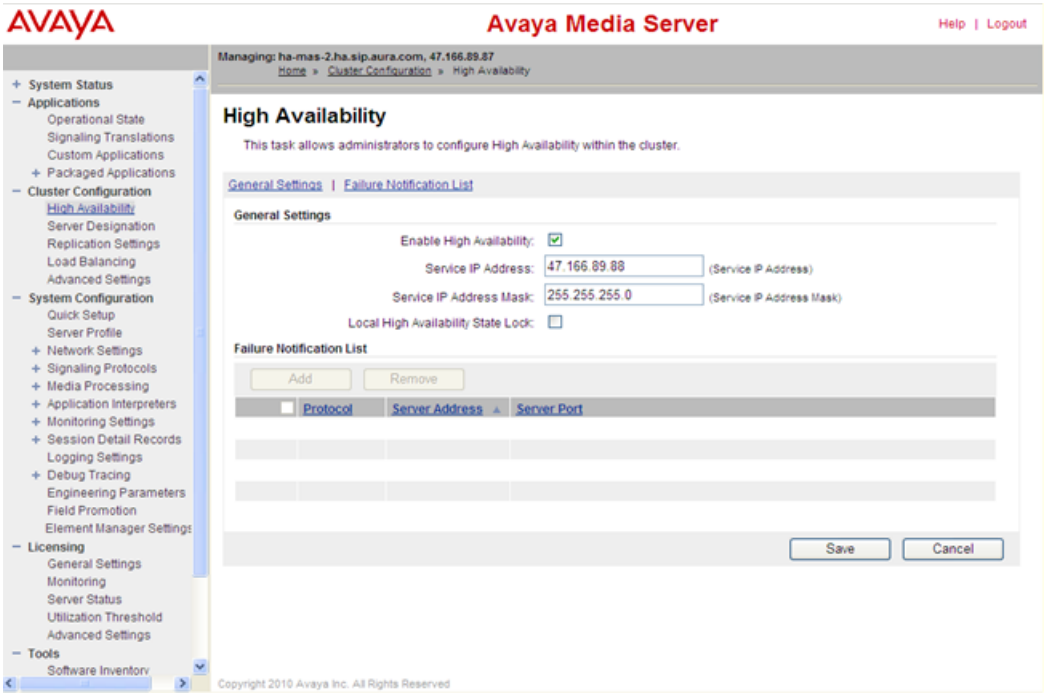


Figure 16: Example of Avaya Media Server High Availability backup server

Configuring the High Availability pair backup Avaya Media Server

Before you begin

- Access the Element Manager for the backup Avaya Media Server.

About this task

Designate the backup server of the high availability pair, configure it with the primary server UUID and IP address, and enter the replication account details.

If you have more than one Avaya Media Server High Availability pair, select one server from each Avaya Media Server pair to be the backup Avaya Media Server server. Perform this procedure on the backup Avaya Media Server of each High Availability pair.

Procedure

1. In the backup Avaya Media Server Element Manager navigation pane, click **Cluster Configuration**.
2. Select **Server Designation**.
3. Under **Local Servers**, select **Backup** from the **Role** list.
4. Under **Server Designation**, in the **Primary Server UUID** box, type the UUID of the Primary server.
5. Type the primary server IP address in the **Primary Server Address** box.
6. Under **Replication Account**, select the **Enable Replication Account** check box.
7. In the **Username** box, type the username for the replication account that you specified on the primary server.
8. In the **Password** box, type the password for the replication account that you specified on the primary server.
9. Click **Save**.

Procedure job aid

Configure the backup Avaya Media Server to enter the primary server UUID and IP address, and the replication account for the High Availability pair.

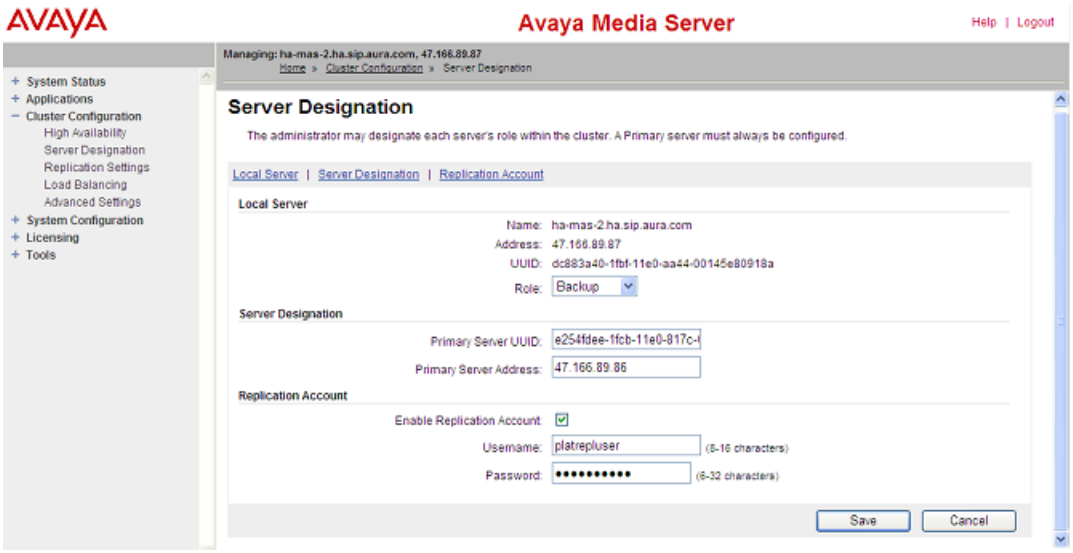


Figure 17: Example of designating an Avaya Media Server as a backup server

Adding the license file to the primary Avaya Media Server

Before you begin

- Obtain an Avaya Media Server license key from Avaya.
- Access the Element Manager for the primary Avaya Media Server.

About this task

Add the license file to the primary Avaya Media Server. The backup Avaya Media Server replicates the license from the primary server.

Note:

If you are using WebLM licensing, skip this procedure.

If you have more than one Avaya Media Server High Availability pair, select one server from each Avaya Media Server pair to be the primary Avaya Media Server server. In each High Availability Avaya Media Server pair, the license file must contain the MAC addresses of both the primary and the backup servers of that High Availability pair. Configure the primary Avaya Media Server of each High Availability pair as the license server.

Perform this procedure on the primary Avaya Media Server of each High Availability pair.

Procedure

1. In the primary Avaya Media Server Element Manager navigation pane, click **Licensing**.
2. Click **General Settings**.

3. Select License Server from the **Licensing** list.
4. In the **Replace License Keys** box, paste the license key for this high availability pair.
5. Click **Validate**.
   The Avaya MS validates the key and displays the licenses in the license details list. The list shows each license type twice, one entry for each MAC address.
6. Click **Save**.

Restarting the primary and backup servers

About this task

Restart both servers so that the backup server can begin replicating from the primary server. Ensure that the primary server is fully operational before starting the backup server.

Procedure

1. Shut down the backup server.
2. Perform an operating system restart on the primary server.
3. When the primary server is fully operational, start the backup server.

Configuring Content Store replication across multiple Avaya Media Server High Availability pairs

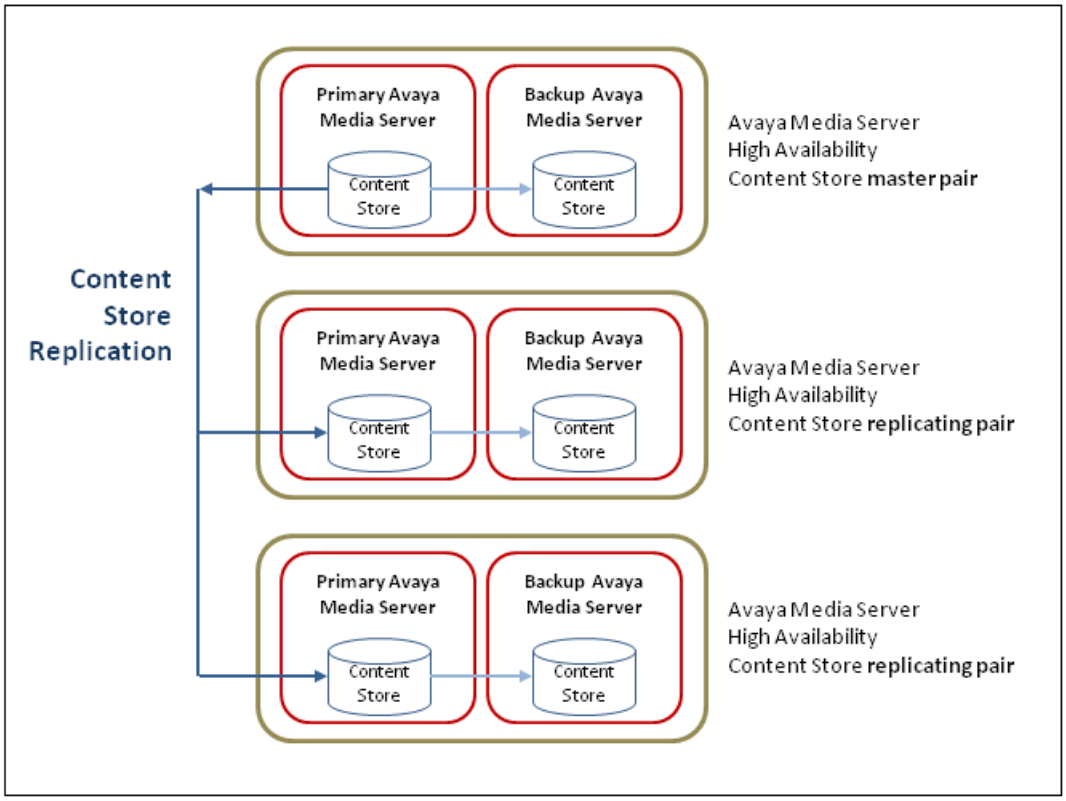
About this task

In a solution with more than one Avaya Media Server High Availability pair, select one of the Avaya Media Server High Availability pairs to be the Content Store master pair. Then configure the other Avaya Media Server High Availability pairs to replicate the media from this Content Store master pair.

You use the Element Manager of the Avaya Media Server Content Store master pair to configure Content Store media such as dialog prompts (announcements) and music. The Content Store media updates and changes you make on the Content Store master pair are then replicated to the other Avaya Media Server High Availability Content Store replicating pairs.

The following diagram shows two Avaya Media Server High Availability Content Store replicating pairs duplicating Content Store media from the Avaya Media Server High Availability

Content Store master pair.



Select one of the Avaya Media Server High Availability pairs to be the Content Store master pair and then configure all the other primary Avaya Media Server servers to replicate the Content Store media from the Content Store master pair.

Perform this procedure on all primary Avaya Media Server High Availability servers, except for the Avaya Media Server Content Store master pair, to configure each Avaya Media Server High Availability replicating pair to replicate Content Store master media data from the Content Store master.

⚠ Caution:

Do not perform this procedure on the Avaya Media Server High Availability Content Store master pair.

Procedure

1. Log on to an Avaya Media Server High Availability Content Store replicating pair primary Element Manager.
2. In the navigation pane, click **Cluster Configuration**.
3. Click **Replication Settings**.
4. In the **Master Cluster Primary Node Address** box, type the IP address for the primary Avaya Media Server of the High Availability Content Store master pair.
5. Click **Save**.

6. Repeat this procedure for each Avaya Media Server High Availability Content Store replicating pair.

Configuring Content Store replication to an Avaya Media Server cluster at a remote site

Before you begin

- Select one of the (local site) campus Avaya Media Server High Availability pairs to be the Avaya Media Server High Availability Content Store master pair.
- Install the Avaya Media Server(s) at the remote site.

About this task

Configure the primary server of an Avaya Media Server cluster (or a standalone Avaya MS) at a remote site to replicate from a high availability pair at the campus site. This allows the administrator to perform Content Store configuration on the active server of a single pair at the campus, and the replication copies this to the primary Avaya MS server at the remote site.

⚠ Caution:

Do not perform this procedure on the Avaya Media Server High Availability Content Store master pair.

Procedure

1. Log on to the Element Manager for the primary Avaya Media Server on the remote site that you want to have replicate from the Avaya Media Server High Availability Content Store master pair.
2. In the navigation pane, click **Cluster Configuration**.
3. Select **Replication Settings**.
4. In the **Master Cluster Primary Node Address** box, type the IP address of the primary Avaya Media Server campus High Availability Content Store master pair.
5. Click **Save**.

Chapter 8: Avaya Media Server common commissioning

This chapter includes commissioning procedures for Avaya Media Server (Avaya MS) in a SIP-enabled contact center.

Avaya Aura® Contact Center uses the media processing capabilities of the Avaya Media Server – Contact Center Services component to support conferencing, announcements, and dialogs in SIP-enabled contact centers.

Configuring media on the Avaya Media Server

Avaya MS provides default media for standard ringback and busy tones in a SIP-enabled contact center. Contact Center uses these default tones with SIP-based phone calls.

Administrators provision additional media such as recorded announcements (RAN) and music for Avaya MS to provide meaningful treatments to the customer.

Media file formats

Avaya MS provides optimum playback performance with .WAV files encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec. Create your announcement and music media files with this encoding before copying them onto the Avaya MS server.

Media organization

In Avaya MS Element Manager (EM), you organize media within a content namespace. The content namespace name must match the contact center SIP domain name; that is, the Local SIP Subscriber Domain Name in Contact Center Manager Server – Server Configuration.

Within the content namespace you use content groups to subdivide the media into logical groups. You must create one locale-specific content group for treatments such as RAN. The locale-specific content group must match the Local SIP Subscriber MS Locale in Contact Center Manager Server – Server Configuration.

You can create one or more additional content groups for music. Typically you store different types of music media in different content groups.

To use recorded announcement (RAN) blocks in Orchestration Designer (OD) flow applications, you create routes in Contact Center Manager Administration (CCMA) that link to the media files in the Avaya MS locale-specific content group. To use scripted music in OD flow applications or scripts, you create routes in CCMA that link to the Avaya MS content groups

containing the music files. The OD flow applications or scripts reference these routes to access the treatment files and scripted music on the Avaya MS server.

The following example shows the structure of a content namespace for a contact center based in Canada, which uses both English and French Canadian recorded announcements, and has three optional music types; folk, jazz, and rock. The SIP domain for the contact center is sipaacc.com. The locale configured on the CCMS server is en_ca.

The media content namespace structure is as follows:

sipaacc.com <= media content namespace, matches SIP domain

| en_ca <= locale-specific media content group (announcements)

| folk <= media content group (folk music)

| jazz <= media content group (jazz music)

| rock <= media content group (rock music)

Even though this example contact center implements announcements in two languages, there is only one locale-specific content group, and this matches the locale configured on the CCMS server. All announcements for both French and English must be stored under the en_ca folder. These can be named: greeting.wav and greeting_fr.wav.

Continuous streaming media

Avaya Media Server supports the configuration of a continuously streamed source for music. To use continuous streamed source, you can configure either a Really Simple Syndication (RSS) URL or a SHOUTCast URL from which the Avaya Media Server can provide music to the Contact Center.

Avaya recommends using a continuously streamed source of music for scripted music. Using continuously streaming music provides music continuity. Customers hear the same music stream (and music type) before and after announcements and therefore they have a much better assisted experience.

To use streamed music in Contact Center Orchestration Designer flow applications, you create routes in Contact Center Manager Administration (CCMA) that link to the RSS channel or the SHOUTCast Channel Key configured on the Avaya MS server. The OD flow applications reference these routes to access the streamed music.

Avaya Media Server scripted music

Avaya Media Server supports the configuration of a continuously streamed source for scripted music. Configure Avaya Media Server to supply only scripted music treatments inserted in to a voice call by an in Contact Center Orchestration Designer (OD) flow application.

To use streamed music in Contact Center Orchestration Designer (OD) flow applications or scripts, you create routes in Contact Center Manager Administration (CCMA) that link to the RSS channel or the SHOUTCast Channel Key configured on the Avaya Media Server. The OD flow applications or scripts reference these routes to access the streamed music.

If the SHOUTCast music stream is not available, and if a Really Simple Syndication channel matches the SHOUTCast channel key, Avaya Media Server switches to that Really Simple Syndication channel music stream.

Music on hold

Both Communication Manager and Avaya Communication Server 1000 can supply music when agents put a call on hold (music-on-hold). If you configure the Communication Manager or Avaya Communication Server 1000 PABX to supply music-on-hold for agents, do not configure Avaya Media Server to supply music-on-hold. Configure Avaya MS to supply only scripted music treatments inserted in to a voice call by an Orchestration Designer flow application or script.

For more information on how to configure music-on-hold using your Communication Manager, see *Avaya Aura® Communication Manager Feature Description and Implementation.*

Call Force Answer Zip Tone

In a SIP-enabled Contact Center, Avaya Aura® Contact Center 6.2 supports an optional configuration to give Call Force Answer (CFA) Zip Tone to all agents who answer a voice call. A zip tone is a tone or beep that a contact center agent hears before they are connected to a customer call. The restricted CFA Zip Tone Feature provides a global system wide setting that turns CFA Zip Tone on or off for all agents. This is a restricted version of the Call Force Answer Zip Tone feature, as it is not connected with the Call Force option in the call presentation class of your Contact Center Manager Administration (CCMA) configuration.

You can also configure a silence period to fall after the zip tone and before the agent and customer are connected on a call. This silence period is a separate setting to the Call Force Delay Timer setting within the CCMA Call Presentation Class configuration.

Call Force Answer Zip Tone works in conjunction with Agent Greeting. Agent Greeting is delayed until the end of the Call Force Answer Delay period. For more information on how to configure Agent Greeting, see Agent Greeting commissioning on page 261.

This feature presents the customer call to the agent while the agent is still hearing the zip tone and the silence that follows. The agent is connected for the duration of this time. This causes the CCMA reports for the Call Delay Time and Active fields to be inaccurate by the length of time of the zip tone and the Call Force Answer Delay Timer, which is configured in Element Manager.

Prerequisites for Avaya Media Server common commissioning

- Install Avaya Media Server. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- Complete the procedures specific to your contact center deployment type. For more information, see Avaya Media Server commissioning for non-HA deployments on page 47 or Avaya Media Server commissioning for HA deployments on page 57.

- Prepare the media .WAV files for announcements and music, encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec.
- If you are planning to use continuous streamed source to provide music, ensure that the RSS or SHOUTCast server is configured and operational.

Avaya Media Server common commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to configure the Avaya Media Server.

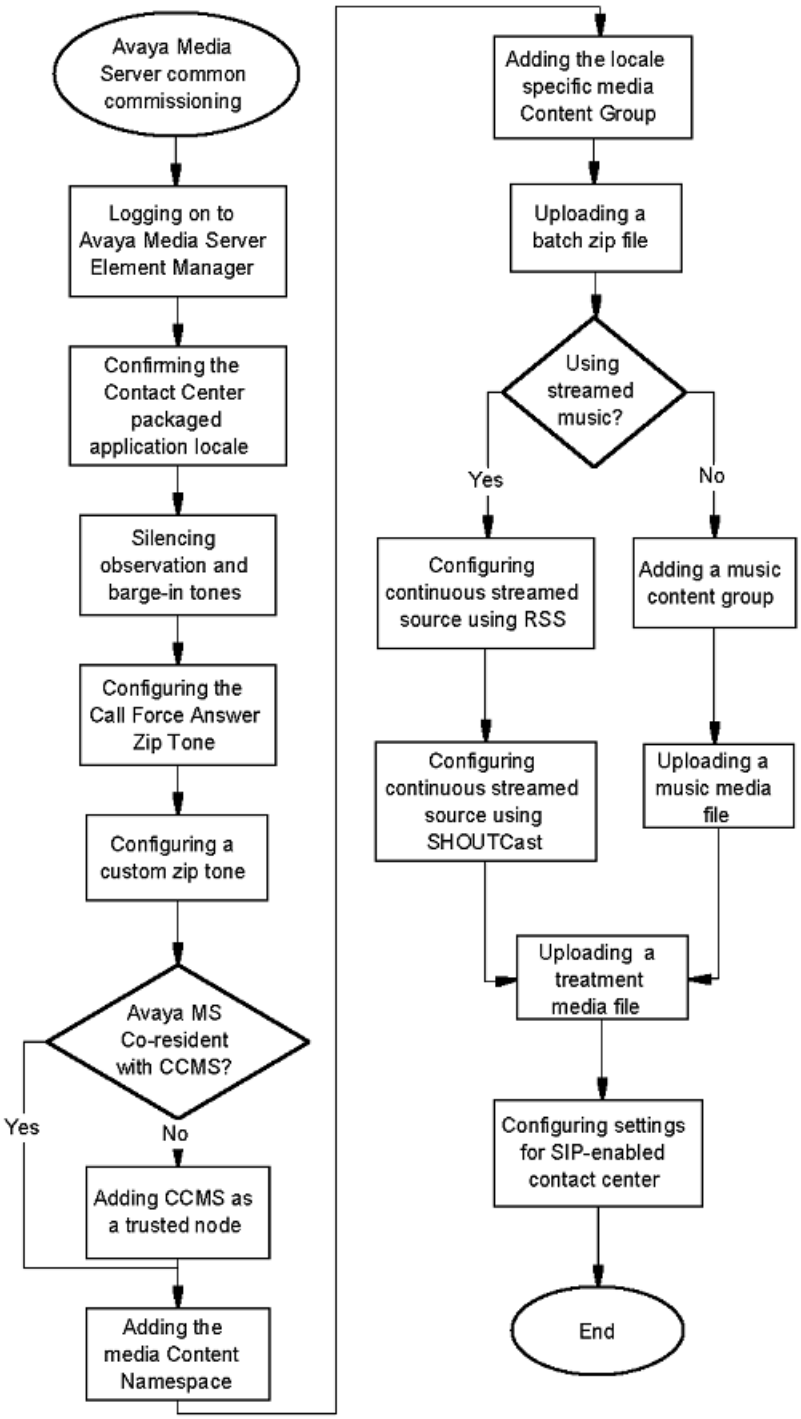


Figure 18: Avaya Media Server common commissioning procedures

Logging on to Avaya Media Server Element Manager

Before you begin

- Obtain a valid user name and password to access Avaya Media Server Element Manager.

About this task

Log on to the Avaya Media Server Element Manager as an administrator to configure Avaya Media Server.

Element Manager (EM) is a web-based administration tool that facilitates the Operation, Administration, and Maintenance (OAM) of Avaya Media Server. A SIP-enabled Contact Center solution must contain one or more Avaya Media Server servers. Each Avaya Media Server server in the Contact Center solution must be licensed and configured to provide media services.

Procedure

1. On the Avaya Media Server server, start a Web browser.
2. In the address box, enter https://SERVER_IP_ADDRESS:8443/em. Where SERVER_IP_ADDRESS is the IP address of the Avaya Media Server.
3. In the **User ID** box, type the Avaya Media Server User ID log on account name. The default Element Manager User ID account name is the Avaya MS server administrator account name. If Avaya Media Server is installed on a Windows server, the default administrator account name is *Administrator*. If Avaya Media Server is installed on a Linux server, the default administrator account name is *root*.
4. In the **Password** box, type the Avaya Media Server Element Manager password. The default Element Manager password is the administrator password for the Avaya MS server.
5. Click **Log in**.

Related topics:

Procedure job aid on page 76

Procedure job aid

On each Avaya Media Server server, the default URL to access Element Manager using a web browser is:

https://localhost:8443/em

Confirming the Contact Center packaged application locale

About this task

Avaya Aura® Contact Center uses the media processing capabilities of the Avaya Media Server–Contact Center Services component to support conferencing, announcements and dialogs in a SIP-enabled contact center. These features are locale-specific.

For example, if the Local SIP Subscriber MS Locale in Contact Center Manager Server–Server Configuration is en_gb, then all locale-specific announcements and tones must use this same locale.

Confirm the locale configuration of the core Contact Center Services Packaged Applications to ensure the contact center receives the correct tones and announcements.

All Avaya Media Servers in a contact center solution must use the same country and language locale.

Note:

Perform this procedure on all primary Avaya Media Servers.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **Applications** > **Packaged Applications** > **Contact Center**.
3. On the **General Settings** page, confirm that the **Default Locale** matches the Local SIP Subscriber MS Locale in Contact Center Manager Server–Server Configuration.

Silencing observation and barge-in tones

About this task

If you want to enable agent-supervisors to silently observe and barge-in on calls, silence the observation and barge-in tones on Avaya Media Server.

Avaya Aura® Contact Center provides observe and barge-in features for voice calls. These actions are performed by agent-supervisors on Avaya Aura® Agent Desktop.

When an agent-supervisor observes a call, the agent and customer hear a tone. This is the default setting on Avaya Media Server. Perform the following procedure to silence the observation and barge-in tones.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **Applications** > **Packaged Applications** > **Contact Center** > **General Settings**.
3. On the **General Settings** page, to silence the barge-in tone for voice calls, clear the **Barge In Tone** check box.
4. To silence the observation tone for voice calls, clear the **Observation Tone** check box.
5. Click **Save**.

Configuring the Call Force Answer Zip Tone

Before you begin

Configure your CCMA call presentation class.

In your CCMA Call presentation class, the Call Force delay timer specifies the length of time the agent phone rings before it is Force Answered. In a contact center where the Agent's phone ringer is disabled and the Call Force Answer Zip Tone is enabled, Avaya recommends setting the Call Force Delay Timer to zero seconds. This reduces the customer wait time before they are connected to an agent. For more information on CCMA call presentation classes, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

About this task

Avaya Aura® Contact Center supports an optional Call Force Answer (CFA) Zip Tone configuration, which provides a zip tone to all agents who answer a voice call. You can configure the CFA Zip Tone feature in the Avaya Media Server Element Manager. The Call Force Answer Delay Timer is also configured in Element Manager.

The zip tone heard by the agent can be customized. For more information, see Configuring a custom zip tone on page 79.

Note:

Perform this procedure on all primary Avaya Media Servers.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **Applications** > **Packaged Applications** > **Contact Center** > **General Settings**.
3. To enable the CFA Zip Tone feature, select the **Call Force Answer Zip Tone** check box.
4. In the **Call Force Answer Delay Timer (sec)** box, type the delay between the zip tone and the agent's conversation with the customer.
5. Click **Save**.

Variable definitions

Name	Description
Call Force Answer Zip Tone	Controls playback of a tone to agents when agents answer a voice call.
Call Force Answer Delay Timer (sec)	The delay (in seconds) between the end of the Call Force Answer Zip Tone and the agent being heard by the customer. This value can be set to a minimum of 0 seconds and a maximum of 5 seconds. Agent Greeting, if configured, is delayed until the end of the Call Force Answer Delay period. The customer continues to hear ringback until after this period.

Configuring a custom zip tone

Before you begin

- Provision a zip tone .WAV file, encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec. The .WAV file must have a minimum duration of one second.
- Name the zip tone .WAV file CallForceAnswerTone.wav.

Important:

The zip tone .WAV file must be named CallForceAnswerTone.wav. This file name is case sensitive.

About this task

Avaya Aura® Contact Center supports an optional Call Force Answer (CFA) Zip Tone configuration, which provides a zip tone to agents who answer a voice call. The zip tone that the agents hear is a default tone. You can customize this default zip tone in Element Manager.

Note:

If your solution has an Avaya Media Server cluster, perform this Content Store procedure only on the primary Avaya Media Server.

Note:

If your contact center solution has a single Avaya Media Server High Availability pair, perform this Content Store procedure only on the primary Avaya Media Server. If your contact center solution has more than one Avaya Media Server High Availability pair, perform this Content Store procedure only on the Avaya Media Server High Availability Content Store master pair. Avaya Media Server High Availability Content Store replication duplicates this Content Namespace to all other Avaya Media Servers in your solution.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **Tools** > **Media Management**.
3. Under **Content Namespaces**, select the media content namespace and click **Browse**.

   Important:

   This media content namespace must match the Local SIP Subscriber Domain Name in Contact Center Manager Server–Server Configuration.
4. In the left pane, select the content namespace and click **Add Content Group**.
5. In the **Name** box, type `tones`.

   Note:

   This name is case sensitive.
6. Click **Save**.
7. In the left pane, select **tones** and click **Add Media**.
   Avaya MS displays the Add Media dialog.
8. On the **Add Media** dialog box, click **Browse** and navigate to the file to upload.
9. Select the **Cut extension** check box.
10. Leave the **New Name** box clear.
11. Click **Upload**.

Adding Contact Center Manager Server as a trusted node

About this task

Add the Contact Center Manager Server as a trusted node to Avaya Media Server. This permits Contact Center Manager Server to use the Avaya Media Server services.

You do not need to complete this procedure if Avaya MS is co-resident on the CCMS server.

Note:

Perform this procedure on every primary Avaya Media Server.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **System Configuration** > **Signaling Protocols** > **SIP**.
3. Click **Nodes and Routes**.
4. Click the **Trusted Nodes** link.
5. Click **Add**.
6. On the **Add SIP Trusted Node** page, in the **Host or Server Address** box, type the IP address of the Contact Center Manager Server. If the Contact Center Manager Server uses the High Availability feature, type the managed IP address of the Contact Center Manager Server High Availability pair.
7. Click **Save**.

Adding the media content namespace

About this task

Using the Avaya Media Server Element Manager, add a Content Namespace to the Avaya Media Server Content Store. You use a Content Namespace to store your custom dialog prompts and music media. You can then write Contact Center Orchestration Designer (OD) applications that use your custom media files stored in this Content Namespace. The Content Namespace name must match the contact center SIP domain name; that is, the Local SIP Subscriber Domain Name in Contact Center Manager Server – Server Configuration.

Note:

If your solution has an Avaya Media Server cluster, perform this Content Store procedure only on the primary Avaya Media Server.

Note:

If your solution has a single Avaya Media Server High Availability pair, perform this Content Store procedure only on the primary Avaya Media Server. If your contact center solution has more than one Avaya Media Server High Availability pair, perform this Content Store procedure only on the Avaya Media Server High Availability Content Store master pair. Avaya Media Server High Availability Content Store replication duplicates this Content Namespace to all other Avaya Media Servers in your solution.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **Tools** > **Media Management**.
3. On the **Media Management** page, under **Content Namespaces**, click **Add**.
4. In the **Name** box, type the name for the content namespace.

   Important:

   This media content namespace must match the Local SIP Subscriber Domain Name in Contact Center Manager Server–Server Configuration.
5. Click **Save**.

Adding the locale-specific media content group

Before you begin

- Create the media content namespace. For more information about adding a Content Namespace, see Adding the media content namespace on page 81.

About this task

Using the Avaya Media Server Element Manager, add a locale specific content group to your Content Namespace in the Avaya Media Server Content Store. You use a locale-specific content group to organize your locale-specific custom dialog prompts and music media.

Note:

If your solution has an Avaya Media Server cluster, perform this Content Store procedure only on the primary Avaya Media Server.

Note:

If your solution has a single Avaya Media Server High Availability pair, perform this Content Store procedure only on the primary Avaya Media Server. If your contact center solution has more than one Avaya Media Server High Availability pair, perform this Content Store procedure only on the Avaya Media Server High Availability Content Store master pair. Avaya Media Server High Availability Content Store replication duplicates this Content Namespace to all other Avaya Media Servers in your solution.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **Tools** > **Media Management**.
3. On the **Media Management** page, under **Content Namespaces**, select the content namespace.
4. Click **Browse**.
   Avaya MS displays the Provision Media page.
5. On the **Provision Media** page, in the left pane, select the content namespace.
6. Click **Add Content Group**.
   Avaya MS displays the New Content Group page.
7. In the **New Content Group** dialog box, in the **Name** box, type the name for the locale-specific content group.

   Important:

   This content group must match the Local SIP Subscriber MS Locale in Contact Center Manager Server–Server Configuration.
8. Click **Save**.

Uploading a batch zip file

Before you begin

- Add the content namespace. For more information about adding the Content Namespace, see Adding the media content namespace on page 81.
- Create the media files for a Content Namespace on your local system. You must organize the media files in the required file structure. Then zip the media files.

Important:

You must give the root directory the same name as the content namespace name.

About this task

You can upload a batch file to provision multiple media files on the Avaya Media Server in a single step. This can include all the media to provide call treatments such as announcements or music.

You can provision the media in a content namespace by using one ZIP file for the whole content namespace or by creating one content group at a time. After you upload the media file, Element Manager (EM) displays it in a tree view. The root of the tree is the content namespace and individual content groups appear below it. EM displays the content namespace and the content groups in the left pane, and the media files contained in the selected content group in the right pane.

To provision a single media file, see Uploading a treatment media file on page 89.

Note:

If your solution has an Avaya Media Server cluster, perform this Content Store procedure only on the primary Avaya Media Server.

Note:

If your solution has a single Avaya Media Server High Availability pair, perform this Content Store procedure only on the primary Avaya Media Server. If your contact center solution has more than one Avaya Media Server High Availability pair, perform this Content Store procedure only on the Avaya Media Server High Availability Content Store master pair. Avaya Media Server High Availability Content Store replication duplicates this Content Namespace to all other Avaya Media Servers in your solution.

Procedure

1. Log on to Element Manager from the system on which you have created the batch zip file.
2. In the navigation pane, click **Tools** > **Media Management**.
3. On the **Media Management** page, select the check box next to the content namespace to which you want to add the media.
4. Click **Browse**.
   Avaya MS displays the Provision Media page.
5. On the **Provision Media** page, right-click the content namespace and select **Batch File Provision** on the shortcut menu.
6. On the **Batch File Provision** dialog box, click **Browse**, and then navigate to the zip file to upload.
7. Click **Always overwrite file with the same name**.

   OR

   Click **Do not overwrite files with the same name**.
8. Click **Upload**.

Configuring continuous streamed source using RSS

Before you begin

- Ensure that the Really Simple Syndication (RSS) server that you want to use is configured and operational.

About this task

Configure the Avaya Media Server to use an RSS URL to provide continuous streamed source music to the contact center.

To be able to use the streamed music in an OD flow application or script, you must configure and acquire a route for the channel using the Configuration page of CCMA. This route name must match the RSS channel name. For more information, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

To provide music to callers, add or edit a flow application or script to provide scripted music using OD, using the Route Number entered in the Configuration page of CCMA. For more information, see *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (NN44400-510).

Note:

Perform this procedure on every primary Avaya Media Server.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **System Configuration** > **Media Processing** > **General Settings**.
3. Under **Continuous Streaming Sources**, in the **Audio RSS URL** box, type the URL of the RSS server.
4. Click **Save**.

Configuring continuous streamed source using SHOUTCast

Before you begin

- Ensure that the SHOUTCast server that you want to use is configured and operational.

About this task

Configure the Avaya Media Server to use a SHOUTCast URL to provide continuous streamed source music to the contact center.

To provide music to callers, add or edit a flow application or script to provide scripted music using OD, using the Route Number entered in the Configuration page of CCMA. For more information, see *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (NN44400-510).

To be able to use the streamed music in an OD flow application or script, you must configure and acquire a route for the content group using the Configuration page of CCMA. This route name must match the SHOUTCast Channel Key described in the steps below. For more information, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

Note:

Perform this procedure on every primary Avaya Media Server.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **System Configuration** > **Media Processing** > **General Settings**.
3. Under **Continuous Streaming Sources**, in the **SHOUTCast Channel Key** box, type a descriptive name for the channel. This must be 30 characters or less and contain no special characters.
4. In the **SHOUTCast Primary URL** box, type the URL of the primary SHOUTCast server.
5. Optionally, in the **SHOUTCast Backup URL** box, type the URL of the backup SHOUTCast server.
6. Click **Save**.

Comments? infodev@avaya.com

Adding a media content group

Before you begin

- Create the media content namespace. For more information about adding a Content Namespace, see Adding the media content namespace on page 81.

About this task

Add a content group to contain music media. You can add multiple media content groups to a content namespace. A music content group typically contains music of one category, for example instrumental or jazz music. Contact Center uses music media to provide scripted music in Contact Center Orchestration Designer (OD) flow applications or scripts.

Note:

Skip this procedure if Avaya Media Server uses a continuous streamed music source.

Note:

If your solution has an Avaya Media Server cluster, perform this Content Store procedure only on the primary Avaya Media Server.

Note:

If your solution has a single Avaya Media Server High Availability pair, perform this Content Store procedure only on the primary Avaya Media Server. If your contact center solution has more than one Avaya Media Server High Availability pair, perform this Content Store procedure only on the Avaya Media Server High Availability Content Store master pair. Avaya Media Server High Availability Content Store replication duplicates this Content Namespace to all other Avaya Media Servers in your solution.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **Tools** > **Media Management**.
3. On the **Media Management** page, under **Content Namespaces**, select the content namespace.
4. Click **Browse**.
   Avaya MS displays the Provision Media page.
5. On the **Provision Media** page, in the left pane, select the content namespace.
6. Click **Add Content Group**.
   Avaya MS displays the New Content Group page.
7. In the **New Content Group** dialog box, in the **Name** box, type a name for the new content group.

8. Click **Save**.

Uploading a music media file

Before you begin

- Upload the music .WAV file, encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec, to a folder on the Avaya MS server.
- Add a content namespace. For more information about adding a content namespaces, see Adding the media content namespace on page 81.
- Add a content group. For more information about adding a content group, see Adding a media content group on page 87.

About this task

Upload a music file to provision music for the Avaya Media Server. The music file is used to provide scripted music from an Orchestration Designer (OD) flow application or script.

To be able to use the music in an OD flow application or script, you must configure and acquire a route for the content group using the Configuration page of CCMA. This route name must match the content group described in the steps below. For more information, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

To provide music to callers, add or edit a flow application or script to provide scripted music using OD, using the Route Number entered in the Configuration page of CCMA. For more information, see *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (NN44400-510).

Note:

Skip this procedure if Avaya Media Server uses a continuous streamed music source.

Note:

If your solution has an Avaya Media Server cluster, perform this Content Store procedure only on the primary Avaya Media Server.

Note:

If your solution has a single Avaya Media Server High Availability pair, perform this Content Store procedure only on the primary Avaya Media Server. If your contact center solution has more than one Avaya Media Server High Availability pair, perform this Content Store procedure only on the Avaya Media Server High Availability Content Store master pair. Avaya Media Server High Availability Content Store replication duplicates this Content Namespace to all other Avaya Media Servers in your solution.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **Tools** > **Media Management**.
3. On the **Media Management** page, select the check box next to the content namespace.
4. Click **Browse**.
   Avaya MS displays the Provision Media page.
5. On the **Provision Media** page, expand the content namespace.
6. Select the content group to which you want to add a music file.
7. Click **Add Media**.
   Avaya MS displays the Add Media dialog.
8. In the **Add Media** dialog box, click **Browse** and navigate to the music file on the server.
9. Click **Upload**.

Uploading a treatment media file

Before you begin

- Upload the treatment .WAV file, encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec, to a folder on the Avaya MS server.
- Add the content namespace. For more information about adding a content namespace, see Adding the media content namespace on page 81.
- Add the locale-specific content group. For more information about adding a content group, see Adding the locale-specific media content group on page 82.

About this task

Using Avaya Media Server Element Manager, upload a media file to provide call treatments, such as announcements. Treatment media files must be stored in the locale-specific content group that matches the locale of the contact center.

To be able to use the treatment in an OD flow application or script, you must configure and acquire a route for the treatment file using the Configuration page of CCMA. This route name must exactly match the treatment file described in the steps below. For more information, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

To provide treatments to callers, add or edit a flow application or script to provide treatments using OD, using the Route Number entered in the Configuration page of CCMA. For more

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

Note:

Skip this procedure if Avaya Media Server uses a continuous streamed music source.

Note:

If your solution has an Avaya Media Server cluster, perform this Content Store procedure only on the primary Avaya Media Server.

Note:

If your solution has a single Avaya Media Server High Availability pair, perform this Content Store procedure only on the primary Avaya Media Server. If your contact center solution has more than one Avaya Media Server High Availability pair, perform this Content Store procedure only on the Avaya Media Server High Availability Content Store master pair. Avaya Media Server High Availability Content Store replication duplicates this Content Namespace to all other Avaya Media Servers in your solution.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **Tools** > **Media Management**.
3. On the **Media Management** page, select the check box next to the content namespace to which you want to add treatment media.
4. Click **Browse**.
   Avaya MS displays the Provision Media page.
5. On the **Provision Media** page, expand the content namespace.
6. Select the locale-specific content group.
7. Click **Add Media**.
   Avaya MS displays the Add Media dialog.
8. In the **Add Media** dialog box, click **Browse** and navigate to the media file on the server.
9. Click **Upload**.

Configuring Avaya Media Server settings for SIP-enabled contact center

About this task

Configure the Avaya Media Server settings to ensure Avaya Media Server can provide the optimal service for the Contact Center application.

Note:

Perform this procedure on every primary Avaya Media Server.

Procedure

1. Log on to Element Manager.
2. In the navigation pane, click **System Configuration** > **Media Processing** > **Media Security**.
3. On the **Media Security** page, from the **Security Policy** list, select **Security Disabled**.
4. Click **Save**.
5. In the navigation pane, click **System Configuration** > **Media Processing** > **Video Codecs**.
6. On the **Video Codecs** page, remove all codecs.
7. Click **Save**.
8. In the navigation pane, click **System Configuration** > **Media Processing** > **Audio Codecs**.
9. On the **Audio Codecs** page, ensure that the codecs you want to support appear in the **Enabled** list.
10. Click **Save**.
11. In the navigation pane, click **System Configuration** > **Media Processing** > **Digit Relay (DTMF)**.
12. On the **Digit Relay (DTMF)** page, enable **RFC2833**.
13. On the **Digit Relay (DTMF)** page, enable **INFO digits**. You must enable INFO digits after enabling RFC2833; RFC2833 must appear first on the list.
14. Click **Save**.
15. In the navigation pane, click **System Configuration** > **Media** > **General Settings**.
16. On the **General Settings** page, clear the **QoS Monitoring** check box.

17. Click **Save**.

Chapter 9: Avaya Media Server language commissioning

This chapter describes how to commission additional languages in a SIP-enabled contact center. You select the default location and language (locale) at install time and add support for the additional language(s) during commissioning. The chapter describes how to use Avaya Media Server media files with an Orchestration Designer *Play and Collect* flow application.

Avaya Media Server provides default media for standard ringback and busy tones in a SIP-enabled contact center. Contact Center uses these default tones with SIP-based phone calls. Administrators provision additional media such as recorded announcements (RAN) and music for Avaya Media Server to provide meaningful treatments to the customer.

Media file formats

Avaya Media Server provides optimum playback performance with .WAV files encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec. Create your announcement and music media files with this encoding before copying them onto the Avaya Media Server server.

Media organization

In Avaya Media Server Element Manager (EM), you organize media within a content namespace. The content namespace name must match the contact center SIP domain name; that is, the Local SIP Subscriber Domain Name in Contact Center Manager Server – Server Configuration.

Within the content namespace you use content groups to subdivide the media into logical groups. You must create one locale-specific content group for treatments such as RAN. The locale-specific content group must match the Local SIP Subscriber MS Locale in Contact Center Manager Server – Server Configuration.

Avaya Media Server supports the following locales:

Locale	Language	Country
de_de	German	Germany
en_ca	English	Canada
en_gb	English	United Kingdom
en_ie	English	Ireland
en_in	English	India
en_us	English	United States
es_es	Spanish	Spain
es_mx	Spanish	Mexico

fr_ca	French	Canada
fr_fr	French	France
it_it	Italian	Italy
ja_jp	Japanese	Japan
ko_kr	Korean	Korea
pt_br	Portuguese	Brazil
ru_ru	Russian	Russia
zh_cn	Chinese (Simplified)	China
zh_tw	Chinese (Simplified)	Taiwan

You can create one or more additional content groups for music. Typically you store different types of music media in different content groups. To use recorded announcements (RAN) in Orchestration Designer (OD) flow applications or scripts, you create routes in Contact Center Manager Administration (CCMA) that link to the media files in the Avaya Media Server locale-specific content group. To use scripted music in OD flow applications or scripts, you create routes in Contact Center Manager Administration (CCMA) that link to the Avaya Media Server content groups containing the music files. The OD flow applications or scripts reference these routes to access the treatment files and scripted music on the server.

The following example shows the structure of a content namespace for a contact center based in Canada, which uses both English and French Canadian recorded announcements, and has three optional music types; folk, jazz, and rock. The SIP domain for the contact center is ocs-nmclab.com. The locale configured on the CCMS server is en_ca. All Announcements for both French and English must be stored under the en_ca folder. For example, these can be named: greeting.wav and greeting_fr.wav.

The media content namespace structure is as follows:

ocs-nmclab.com <= media content namespace, matches SIP domain

– en_ca <= locale-specific media content group (announcements)

– folk <= media content group (folk music)

– jazz <= media content group (jazz music)

– rock <= media content group (rock music)

Even though this example contact center implements announcements in two languages, there is only one locale-specific content group, and this matches the locale configured in Contact Center Manager Server.

Default media files

Contact Center Avaya Media Server contains a set of country and language specific default media files for all supported locales. The default media files contain numerical values, busy tones and ring-back tones. You can use these default “canned” media files in your Contact Center solution, or replace them with your own recordings.

The following are examples of the Avaya Media Server default or canned locale specific media files:

- Single digit playback (zero.wav, one.wav, two.wav ... nine.wav)
- Busy tone wav file (busy.wav)
- Ringback wav file (ringback_xx.wav) where xx is the country portion of the locale (for example, ringback_us.wav, ringback_ru.wav)

The default media files are stored in the Operating System file structure (not in the Avaya Media Server content namespace). The canned media files are stored in Linear 16-bit PCM recording format.

If you choose to create your own version of the default media files, you must replace the existing default files with media files of the exact same name. For example, if you choose to record your own numerals, then you must save the files as one.wav and two.wav to match the existing default file names. Then you replace the existing default media files with the media files for your own recordings. You must then reboot the Avaya Media Server server. This forces Avaya Media Server to pick up your most recent Linear 16-bit PCM recording.

Avaya Media Server provides optimum playback performance with .WAV files encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec.

On a Windows operating system Avaya Media Server server, the default location for the default media files is:

```
D:\Avaya\MAS\Multimedia_Applications\MAS\platdata\Announcements
\contactcenter\default\xx\yy\l16
```

Where xx is the country portion of the locale and yy is the language portion of the locale.

For example, the Windows operating system Avaya Media Server directory locations for Canadian English and French are:

```
D:\Avaya\MAS\Multimedia_Applications\MAS\platdata\Announcements
\contactcenter\default\ca\en\l16
```

```
D:\Avaya\MAS\Multimedia_Applications\MAS\platdata\Announcements
\contactcenter\default\ca\fr\l16
```

On a Linux operating system Avaya Media Server server, the default location for the default media files is:

```
/opt/avaya/ma/MAS/platdata/Announcements/contactcenter/default/xx/yy/l16
```

Where xx is the country portion of the locale and yy is the language portion of the locale.

For example, the Linux Operating System Avaya Media Server directory locations for Canadian English and French are:

```
/opt/avaya/ma/MAS/platdata/Announcements/contactcenter/default/ca/fr/l16
```

```
/opt/avaya/ma/MAS/platdata/Announcements/contactcenter/default/ca/en/l16
```

If you did not install Avaya Media Server in the default folder, you can use environmental variables to help you navigate to the media folders.

On a Windows operating system Avaya Media Server server, the location for the default English media files is:

```
%MASHOME%\platdata\Announcements\contactcenter\default\us\en\l16
```

On a Linux operating system Avaya Media Server server, the location for the default English media files is:

```
$MASHOME/platdata/Announcements/contactcenter/default/us/en/l16
```

Prerequisites for Avaya Media Server language commissioning

- Install Avaya Media Server. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- Complete the procedures specific to your contact center deployment type. For more information, see Avaya Media Server commissioning for non-HA deployments on page 47 or Avaya Media Server commissioning for HA deployments on page 57.
- Complete the Avaya Media Server common commissioning procedures. For more information, see Avaya Media Server common commissioning on page 71.
- Prepare the media .WAV files for announcements and music, encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec.

Avaya Media Server language commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to configure additional languages for Avaya Media Server. It also includes procedures on how to use these media files when developing graphical flow applications with Orchestration Designer (OD).

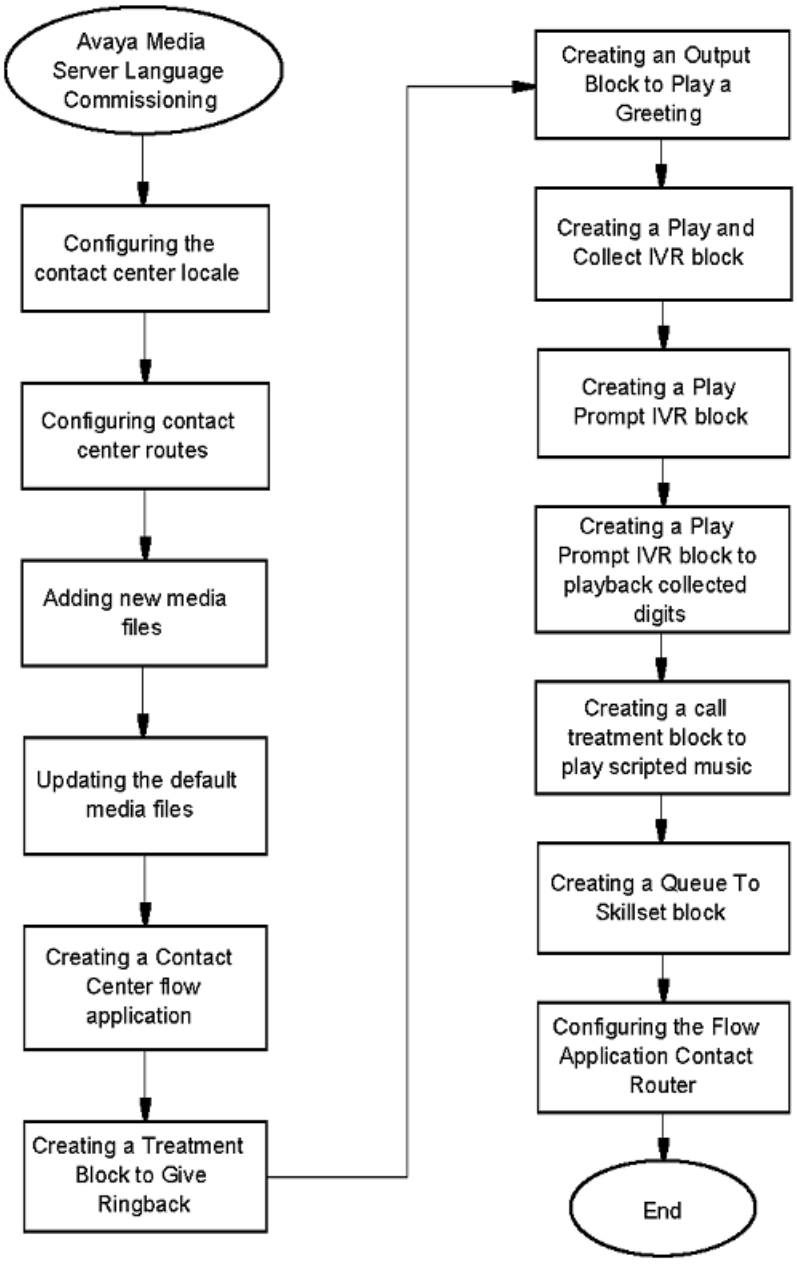


Figure 19: Avaya Media Server additional language commissioning procedures

Configuring the contact center locale

About this task

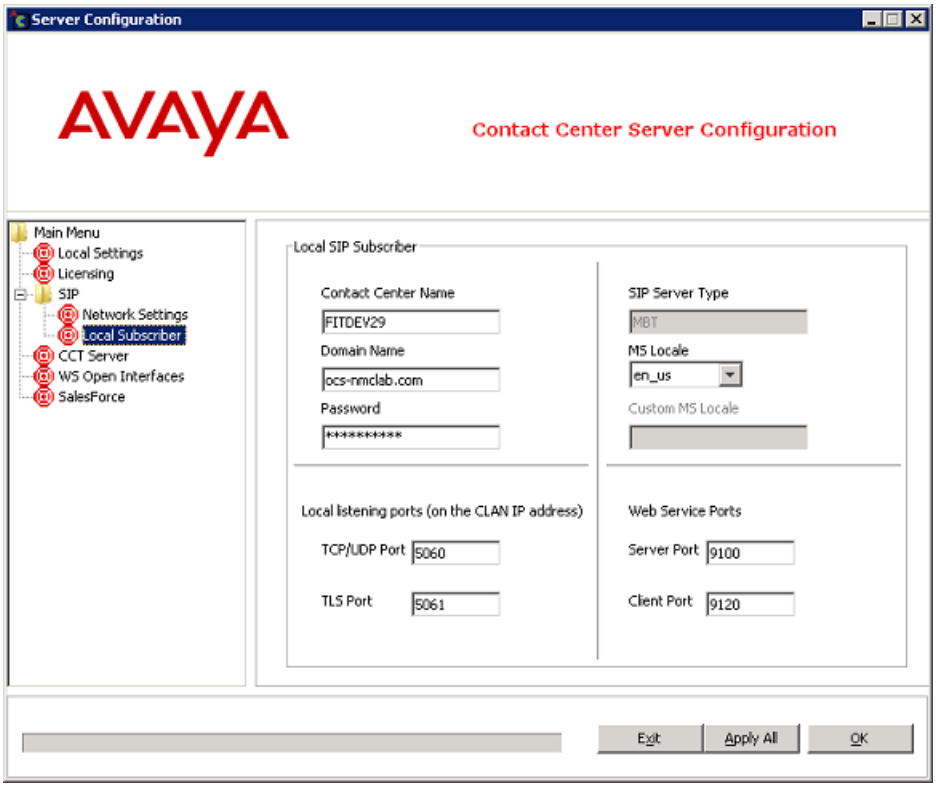
Configure the Contact Center Manager Server media services locale at installation time. Use the Contact Center Manager Server — Server Configuration if you need to change the default media server location during commissioning.

Important:

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

Procedure

1. Log on to the Contact Center Manager Server server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
3. In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.
4. From the **MS Locale** list, select the language and dialect locale of your contact center. This example uses the North American English locale.



5. Click **Apply All**.
6. Click **OK**.
7. Click **Exit**.

Configuring contact center routes

About this task

Routes defined in Contact Center Manager Administration (CCMA) differ depending on the type of PABX to which the Contact Center is attached.

On a SIP-enabled Contact Center (using either an Avaya Aura® Unified Communications platform or a SIP-enabled Avaya Communication Server 1000), a route links announcements and music provided by the Avaya Media Server to the RAN block configured in a Orchestration Designer script.

The Route Name is a string that must be identical to the announcement (WAV) file name or music content group (for example, classical, jazz, easy listening) stored on the Avaya Media Server. For announcements the Route Name must be identical to the announcement (WAV) file name under the locale content group on the Avaya Media Server. If the media file in the Avaya Media Server content namespace has a .WAV extension, then the route name entered

here must also have the full extension as part of the name. For example, if the WAV file in the Avaya Media Server content namespace is “MyGreeting.wav”, then the route name must be “MyGreeting.wav”.

The Route Number can be arbitrary (though it must be unique) and the RAN block in the Orchestration Designer uses this number to identify the file to play. See *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (NN44400-510).

The Orchestration Designer (OD) script uses the Route Number mapping to invoke this file for playback. This configuration allows the announcement file name and music content group to appear on the generated RAN and MUSIC reports.

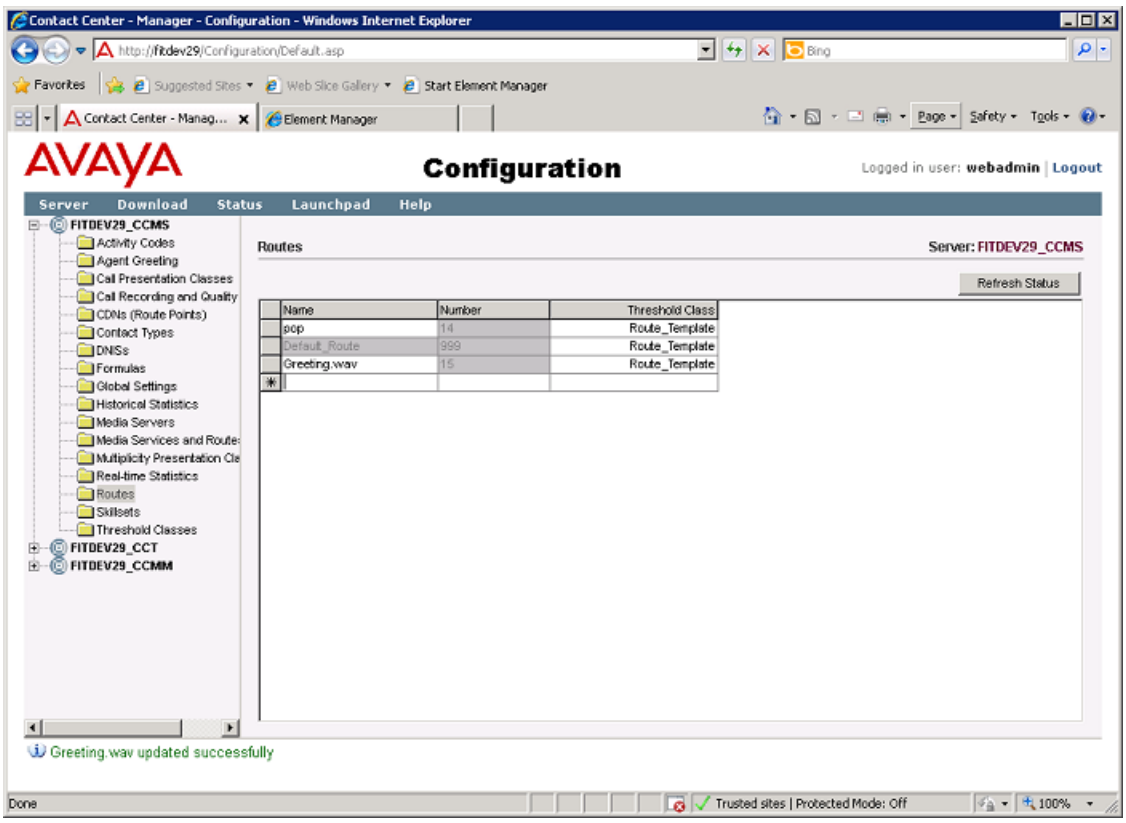
Procedure

1. Start Internet Explorer.
2. In the Address box, type the URL of the Contact Center Manager Administration server. The default URL is http://server name; server name is the computer name of the CCMA server.

   Do not type the IP address in the Address box. Using the IP address results in problems with Scripting, Historical Reporting, Configuration, Contact Center Management, and Access and Partition Management.
3. In the **User ID** box, type your user ID.
4. In the **Password** box, type your password.
5. Click **Login**.
6. On the CCMA **Launchpad**, click **Configuration**.
7. In the left pane, expand the server to which to add the route.
8. Select the **Routes** folder.
9. In the right pane, in the **Name** box, type the name of the route as you want it to appear in reports.
10. In the **Number** box, type the route number.
11. From the **Threshold Class** list, select the threshold class assigned to this route.
12. Click any other row of the table to add the route.

Example

For example, configure two routes. One route to play a greeting to customers (route number 15), and another route to play scripted pop music to customers (route number 14).



Adding new media files

Before you begin

- Upload the treatment .WAV file, encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec, to a folder on the Avaya Media Server.
- Add the content namespace. For more information about adding a content namespace, see Adding the media content namespace on page 81.
- Add the locale-specific content group. For more information about adding a content group, see Adding the locale-specific media content group on page 82.

Important:

To be able to use the treatment in an Orchestration Designer flow application or script, you must configure and acquire a route for the treatment file using the Configuration page in CCMA. This route name must exactly match the treatment file described in the steps below.

Important:

To provide treatments to callers, add or edit a flow application or script to provide treatments using Orchestration Designer, using the Route Number entered in the Configuration page of CCMA.

About this task

Upload a media file to provide call treatments, such as announcements to your primary Avaya Media Server. Treatment media files must be stored in the locale-specific content group that matches the locale of the contact center. If there is more than one Avaya Media Server in your contact center, complete this procedure only on the Primary Avaya Media Server.

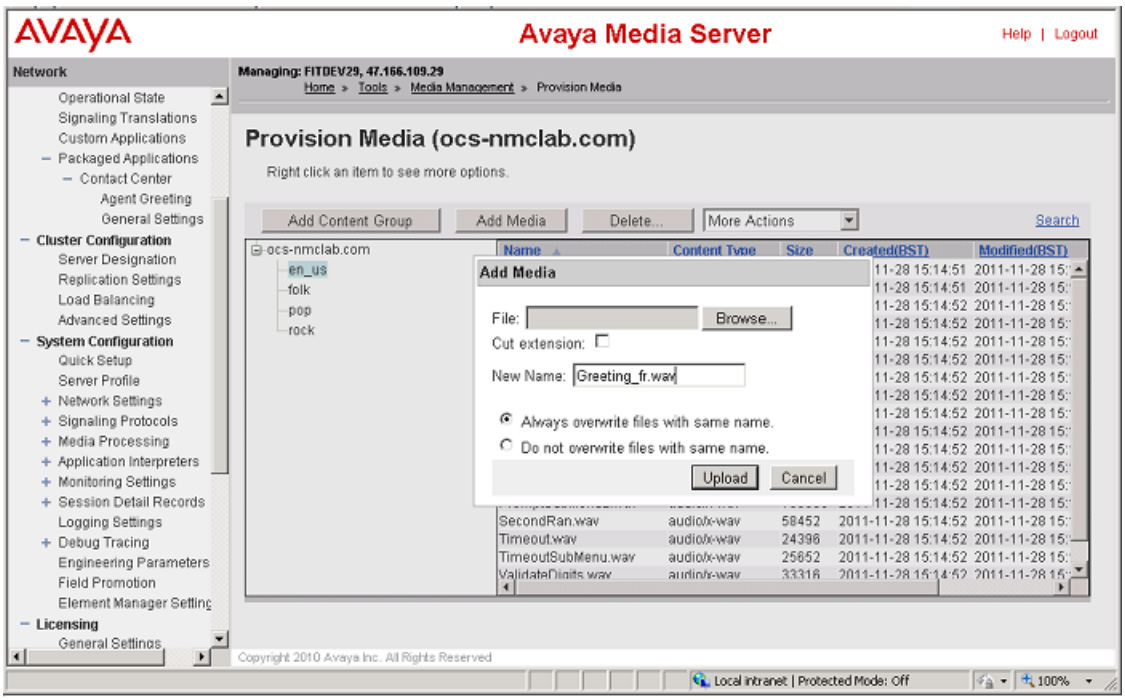
Procedure

1. Log on to Avaya Media Server Element Manager.
2. In the navigation pane, click **Tools** > **Media Management**.
3. On the **Media Management** page, select the check box next to the content namespace to which you want to add treatment media.
4. Click **Browse**.
   Avaya Media Server displays the Provision Media page.
5. On the **Provision Media** page, expand the content namespace.
6. Select the locale-specific content group.
7. Click **Add Media**.
   Avaya Media Server displays the Add Media dialog.
8. In the **Add Media** dialog box, click **Browse** and navigate to the media file on the server.
9. Clear **Cut extension**.
10. Click **Upload**.

Example

For example, add a French language greeting file to the en_us content group.

Example of adding a French greeting media file to Avaya Media Server



Updating the default media files

About this task

Contact Center Avaya Media Server contains a set of country and language specific default media files. The default media files contain numerical values, busy tones and ring-back tones. You can chose to use these default media files in your Contact Center solution, or replace them with your own recordings.

If you choose to create your own version of the default media files, you must replace the existing default files with media files of the exact same name. For example, if you choose to record your own numerals, then you must save the files as one.wav and two.wav to match the existing default file names. Then you replace the existing default media files with the media files for your own recordings. You must then reboot the Avaya Media Server server. This forces Avaya Media Server to pick up your most recent Linear 16-bit PCM recording.

Avaya Media Server provides optimum playback performance with .WAV files encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec

On an Avaya Media Server, the default location for the default US – English media files is:

D:\Avaya\MAS\Multimedia_Applications\MAS\platdata\Announcements\contactcenter\default\us\en\l16

Important:

You must reboot the Avaya Media Server to pickup and use the updated default media files.

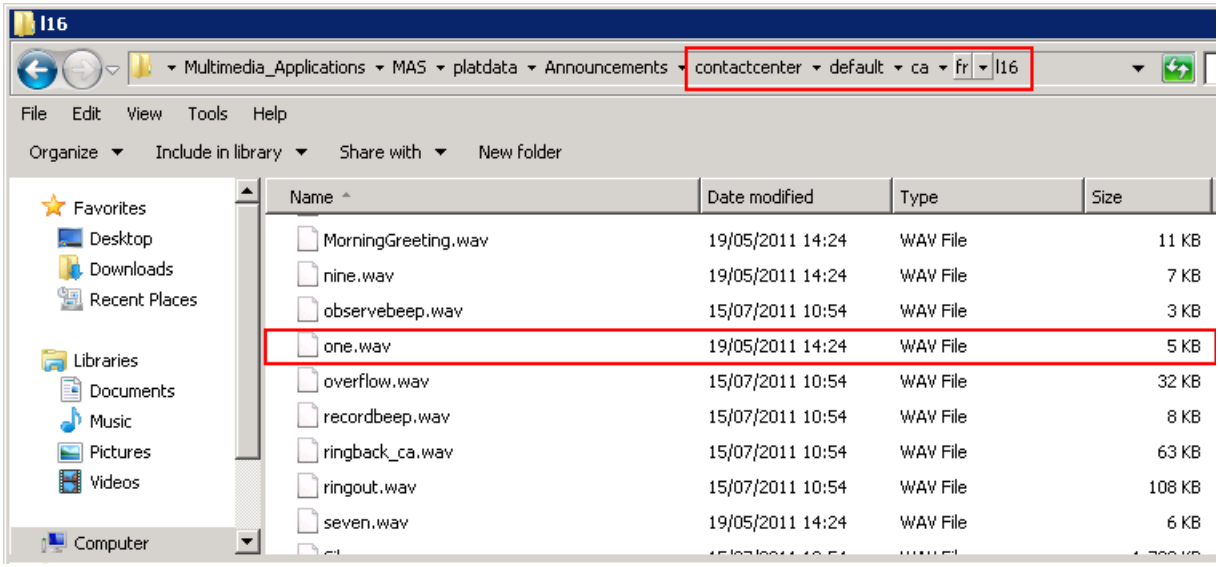
Procedure

1. Generate your own recording of the default recording.
2. Save your recording with the same name as the existing default recording.
3. On the Avaya Media Server, navigate to the folder containing the existing Linear 16-bit PCM default recording.
4. Copy your recording to this folder, overwriting the existing default recording.
5. Reboot the Avaya Media Server server.

Example

For example, replace the Canadian French recording of the number one with your own Canadian French recording of the number one.

Example of updating the Canadian French recording of the number one:



Creating a Contact Center flow application

Before you begin

- Upload the treatment .WAV file, encoded as Linear 16-bit PCM, 8KHz Mono with a sampling rate of 128kbits/sec, to a folder on the Avaya Media Server.

About this task

Using Contact Center Orchestration Designer, create a Contact Center flow application to provide treatments for customer calls. Flow applications use graphical flow chart symbols to define call treatments.

Calls to the Contact Center are routed to a Master application for processing, treatments and queuing to an appropriate skillset. Avaya Aura® Contact Center answers the customer call and executes the Master application, and optional primary and secondary applications.

Applications contain instructions that determine the sequence of steps that a contact follows after the contact arrives at Contact Center. These steps can include call treatments (such as music or ringback), call routing (such as skill-based routing), or interaction with the caller (entering account numbers). Applications perform two major functions: they define the path a contact follows, and they provide treatments to a contact as the contact moves through Contact Center. You can also use the applications to track and record information about each step in the progress of a contact, and use this information to analyze how your contact center functions to improve service.

You use Contact Center Orchestration Designer to create the graphical flow applications. For more information, see *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (NN44400-510).

Procedure

1. Use the Orchestration Designer application to create a flow application.
2. Open Internet Explorer.
3. In the Address box, type http://<Contact Center Manager Administration Server name>
4. Log on to the Contact Center Manager Administration browser as webadmin using the configured password.
5. On the CCMA **Launchpad**, click **Scripting**.
6. Click Orchestration Designer menu, and then click **Launch Orchestration Designer**.
7. Select the **Contact Center** view, if it is not already open in the current view.
8. In the **Contact Center** pane, expand the menu to display the list of applications.
9. Right-click **Applications**, and select **New**, **Application**.

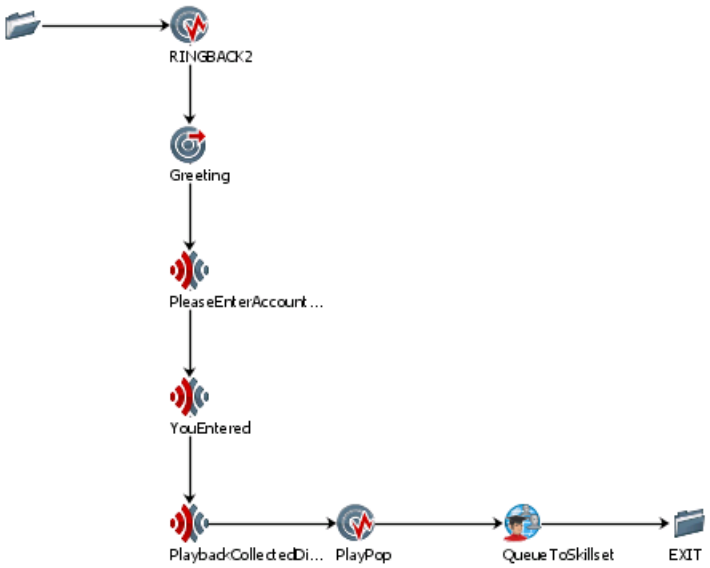
10. In the **New Contact Center Application** dialog box, select **Create in Contact Center**.
11. In the **Application Name** box, type the name of your new flow application. For this example, the name is MyApplication.
12. In **Application Type**, select **Graphical Flow**.
13. In **Application Template**, select **New_Flow**.
14. Click **Finish**. This creates an empty graphical flow application, containing just a Start node and Exit block. You must complete the flow application by adding the IVR blocks, Treatment blocks and Output blocks as detailed in the following procedures.

Example

For example, use Orchestration Designer to create a basic graphical application named MyApplication to:

- Provide ringback to the customer
- Play a greeting to the customer
- Play prompt and collect digits from the customer
- Play confirmation message to the customer
- Play back collected digits, one digit at a time to the customer
- Play some pop music to the customer
- Queue the customer to skillset

Example of a basic graphical application named MyApplication:



Creating a Give Ringback Treatment block

About this task

Create a Give Ringback treatment block to play ringback tones to a customer.

Procedure

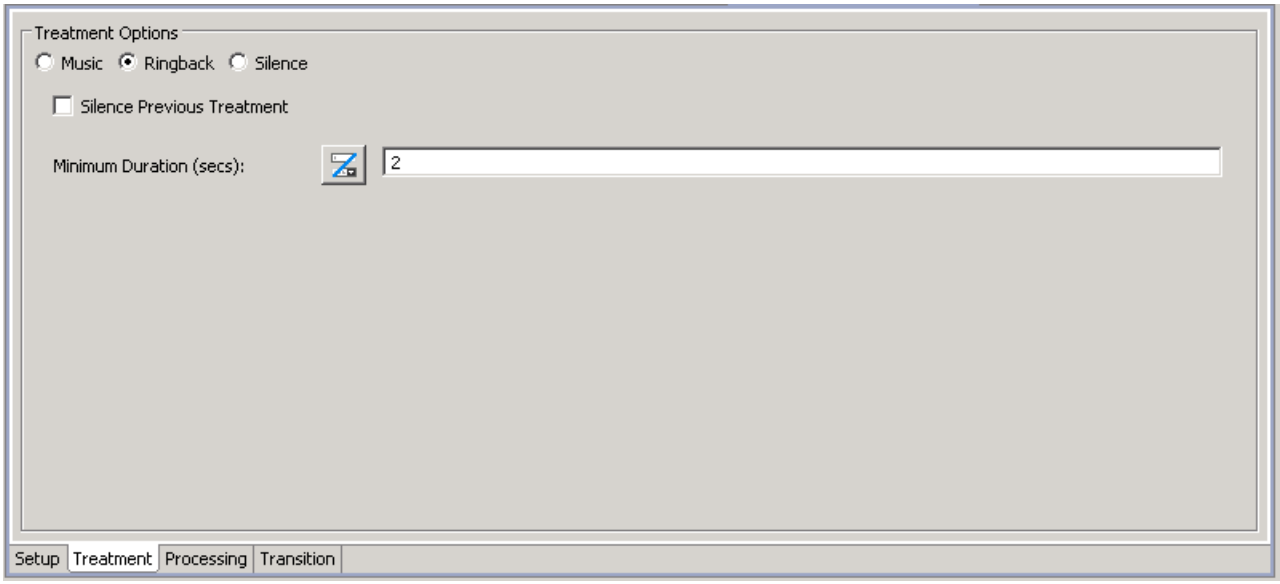
1. In Orchestration Designer, with your flow application open, double-click the treatment block icon.
2. Click the **Setup** tab to configure the general details for the block. Configure RINGBACK2 as the name of this block.
3. Click the **Treatment** tab.
4. Select **Ringback**.
5. In the **Minimum Duration (secs)** box, type the length of time in seconds to play the ringback tone for.
6. Select the Main [MyApplication] flow application view.
7. Left-click the **Start** node and then right-click on the **Exit** block, and select **(Dis)Connect**. The link from the Start node to the Exit block disappears.

8. Left-click the **Start** node and then right-click on the RINGBACK2 block, and select **(Dis)Connect**. This configures this flow application to begin by playing a ringback tone to the customer.

Example

For example, create a treatment block to give ringback for two seconds.

Example of using a treatment block called RINGBACK2 to play ringback tones:



Creating an Output block to play a greeting

About this task

Using Orchestration Designer (OD), create an Output block to play a recorded announcement (RAN) greeting to customers.

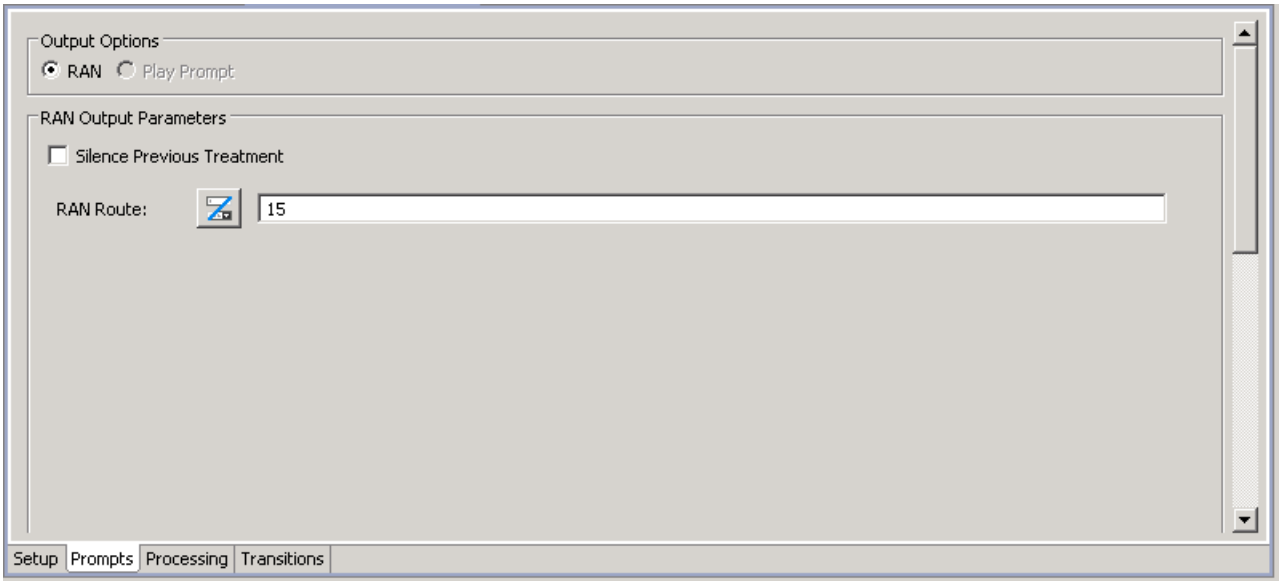
Procedure

1. In Orchestration Designer, with your flow application open, double-click the Output block icon.
2. Click the **Setup** tab to configure the general details for the block. Configure Greeting as the name of this Queue to Output block.
3. Click the **Prompts** tab.
4. Select **RAN**.

5. In the **RAN Route** box, type the route number of the greeting to play the Customer. The RAN Route number must match a route number configured in Contact Center Manager Administration.
6. Select the Main [MyApplication] flow application view.
7. Left-click the RINGBACK2 block and then right-click on the Greeting block, and select **(Dis)Connect**. This connects the output of the RINGBACK2 block with the input of the Greeting block.

Example

For example, use an Output block named Greeting to play a greeting to customers. The route number 15 must match a greeting route number configured in Contact Center Manager Administration.



Creating a Play and Collect IVR block

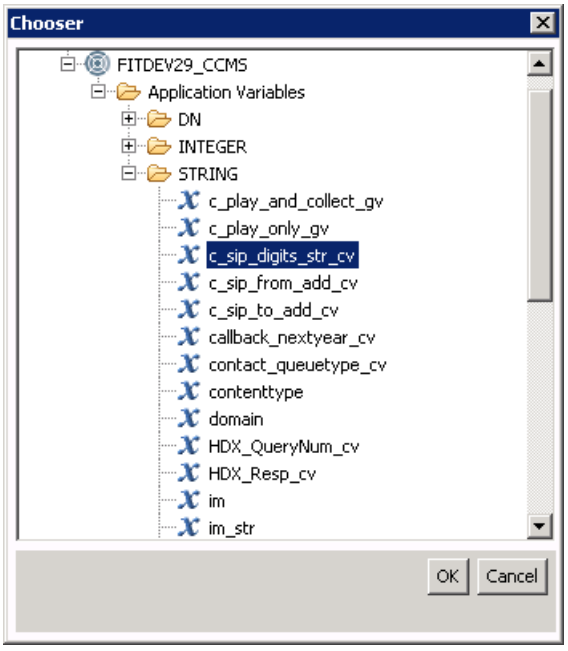
About this task

Using Orchestration Designer (OD), create an Interactive Voice Response (IVR) block to play prompts and collect digits. Create an IVR block to play a prompt to the Customer. For example, play the PlayPrompt.wav media file to ask the customer to enter their account number. The customer then uses the number keypad on their phone to enter their digits. The Play and Collect IVR block collects the Customer digits and stores then in the a string variable. You must use string variables to store digits, especially when the number if longer than 10 digits.

In addition to the main configuration tabs, the IVR block has the IVR tab. Use the IVR tab to configure the properties of the IVR application for your call.

Procedure

1. In Orchestration Designer, with your flow application open, double-click the IVR block icon.
2. Click the **Setup** tab to configure the general details for the block. Configure PleaseEnterAccountNumber as the name of this IVR block.
3. Click the **IVR** tab.
4. Select **Play and Collect**.
5. In the **Prompt Name** box, type the name of the prompt to play the customer. This prompt asks the customer to enter a sequence of digits. For example, enter PlayPrompt.wav.
6. In the **Return Value** box, enter the name of a string variable or click and Browse to select a string variable to use for saving the collected digits. For example, select the c_sip_digits_str_cv string variable. You must use string variables to store digits longer than 10 digits.



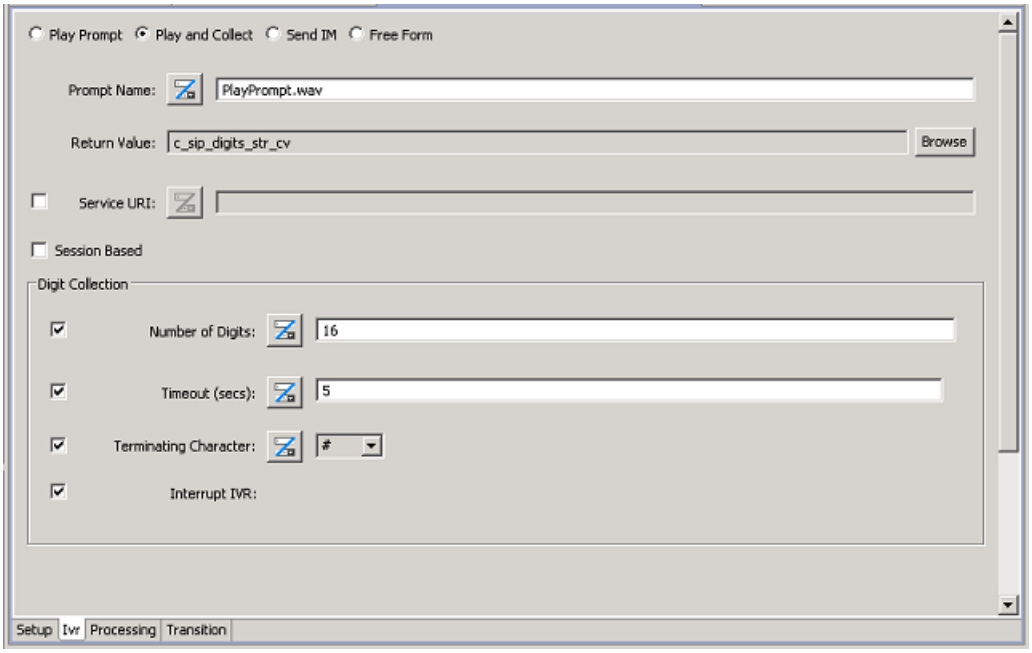
7. Select the **Number of Digits** check box, to allow the user to select the Number of Digits.
8. In the **Number of Digits** box, enter 16 as the maximum number of digits. You may also configure this to accept only the number of digits your voice prompts requests. For example, if your voice prompt asks the customer to enter their five digit account number, then configure this value as five.

9. Select the **Timeout (secs)** check box.
10. In the **Timeout (secs)** box, enter the maximum number of seconds to wait for the customer before you play the Timeout message.
11. Select **Terminating Character**.
12. From the **Terminating Character** list, select #.
13. To be able to interrupt the IVR, select the **Interrupt IVR** check box.
14. Select the Main [MyApplication] flow application view.
15. Left-click the Greeting output block and then right-click on the PleaseEnterAccountNumber block, and select **(Dis)Connect**. This connects the output of the Greeting block with the input of the Play and Collect PleaseEnterAccountNumber block.

Example

For example, add an Interactive Voice Response (IVR) block to your application. Create an IVR block to play a prompt to the customer. For example, play the PlayPrompt.wav media file to ask the customer to enter their account number. The customer then uses the number keypad on their phone to enter their digits. The Play and Collect IVR block collects the customer digits and stores then in the a c_sip_digits_str_cv string variable. You must use string variables to store digits longer than 10 digits.

Example of a Play and Collect IVR Block:



Creating a Play Prompt IVR block

About this task

Using Orchestration Designer (OD), create an IVR block to play a prompt to the Customer. For example, the Play Prompt IVR block may play a validation message to your Customers to confirm the digits they entered.

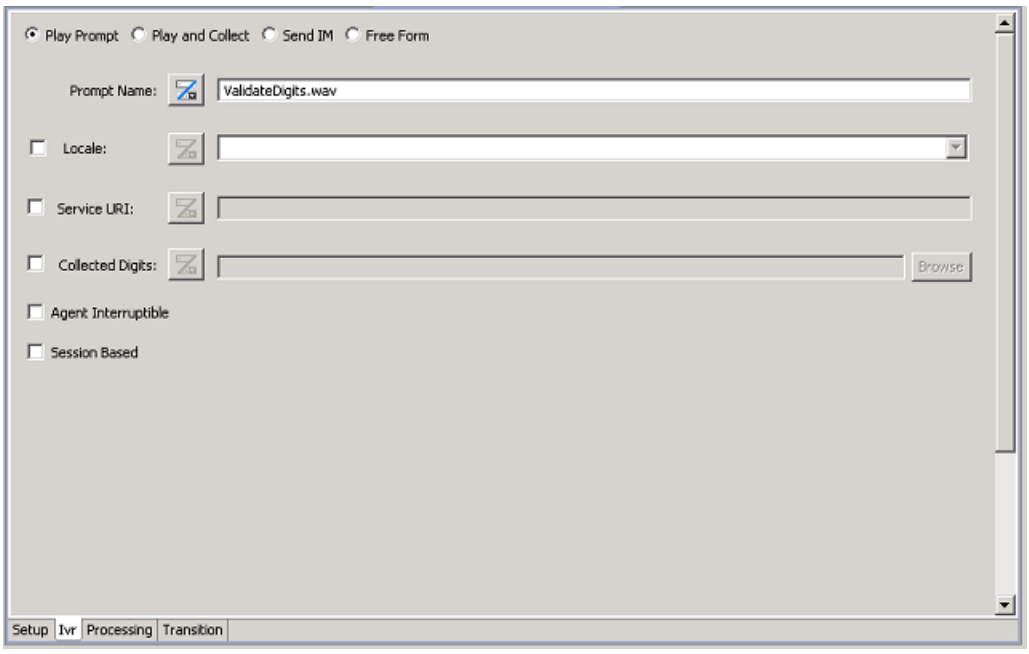
Procedure

1. In Orchestration Designer, with your flow application open, double-click the IVR block icon.
2. Click the **Setup** tab to configure the general details for the block. Configure YouEntered as the name of this IVR block.
3. Click the **IVR** tab.
4. Select **Play Prompt**.
5. In the **Prompt Name** box, type the name of the prompt to play the Customer. For example, enter ValidateDigits.wav.
6. Select the Main [MyApplication] flow application view.
7. Left-click the PleaseEnterAccountNumber IVR block and then right-click on the YouEntered block, and select **(Dis)Connect**. This connects the output of the PleaseEnterAccountNumber IVR block with the input of the YouEntered block

Example

For example, add an IVR block to your application. Create an IVR block to play a prompt to the Customer. For example, play the ValidateDigits.wav media file to the Customer telling them they are about to hear the digits they have just entered. This example does not play back the actual digits, the next IVR block in the application plays back the collected digits.

Example of a Play Prompt IVR Block:



Creating a Play Prompt IVR block to playback collected digits

About this task

Create a Play Prompt IVR block to play back the digits collected digits to the customer. This Play Prompt IVR block uses the French Canadian locale.

Procedure

1. In Orchestration Designer, with your flow application open, double-click the IVR block icon.
2. Click the **Setup** tab to configure the general details for the block. Configure PlayCollectedDigits as the name of this IVR block.
3. Click the **IVR** tab.
4. Select **Play Prompt**.
5. In the **Prompt Name** box, type %i0. This configures the Play Prompt IVR Block – to play back the collected digits as a sequence of digits. For example, if a Customer enters 124, the Play Prompt IVR block plays back “one”, “two”, and “four” (not “one hundred and twenty four”).
6. Select the **Locale** check box.

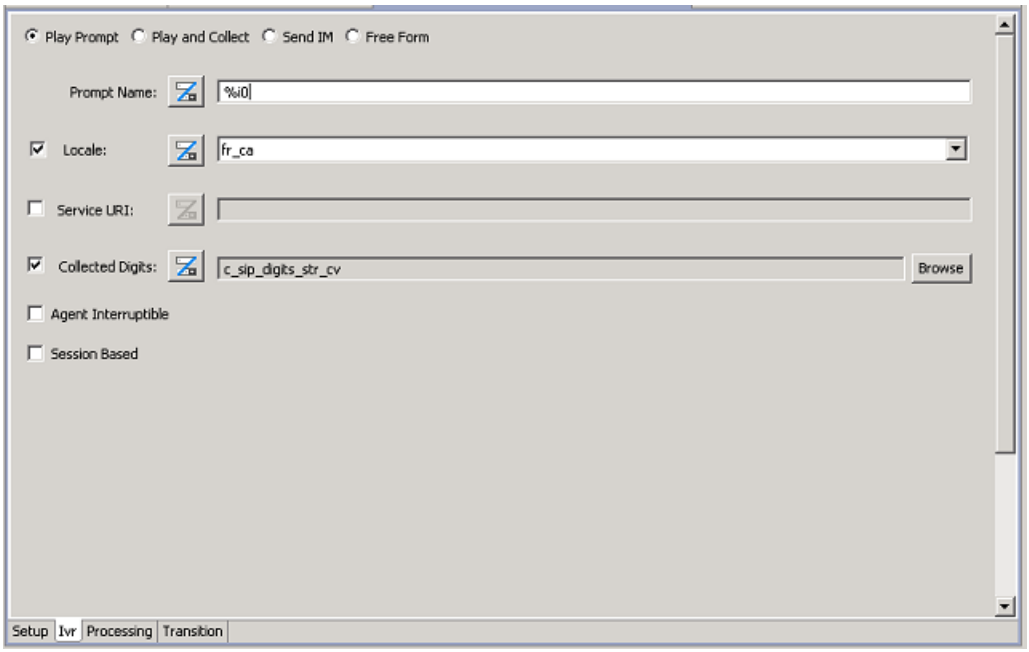
7. From the **Locale** list, select the country and language. For example select Canadian French *fr_ca*. If a Customer enters 124, the Canadian French locale Play Prompt block plays back “un”, “deux”, and “quatre”.
8. Select the **Collected Digits** check box.
9. From the **Collected Digits** list, select the string variable containing the digits collected from the customer earlier.
10. Select the Main [MyApplication] flow application view.
11. Left-click the YouEntered IVR block and then right-click on the PlayCollectedDigits block, and select **(Dis)Connect**. This connects the output of the YouEntered IVR block with the input of the PlayCollectedDigits block.

Example

Example of a Play Prompt IVR block configured to play back the customer entered digits. The digits are played back in the Canadian French language. The Play Prompt IVR block uses the French Canadian locale, so it uses the media files stored at:

```
D:\Avaya\MAS\Multimedia_Applications\MAS\platdata\Announcements
\contactcenter\default\ca\fr\l16
```

If a Customer enters 124, the Canadian French locale Play Prompt block uses the one.wav, two.wav, and four.wav media files to play-back “un, deux, quatre”.



Creating a call treatment block to play scripted music

About this task

Create a treatment block to play scripted music to the customer while they wait in queue. For example, play pop music to the customer.

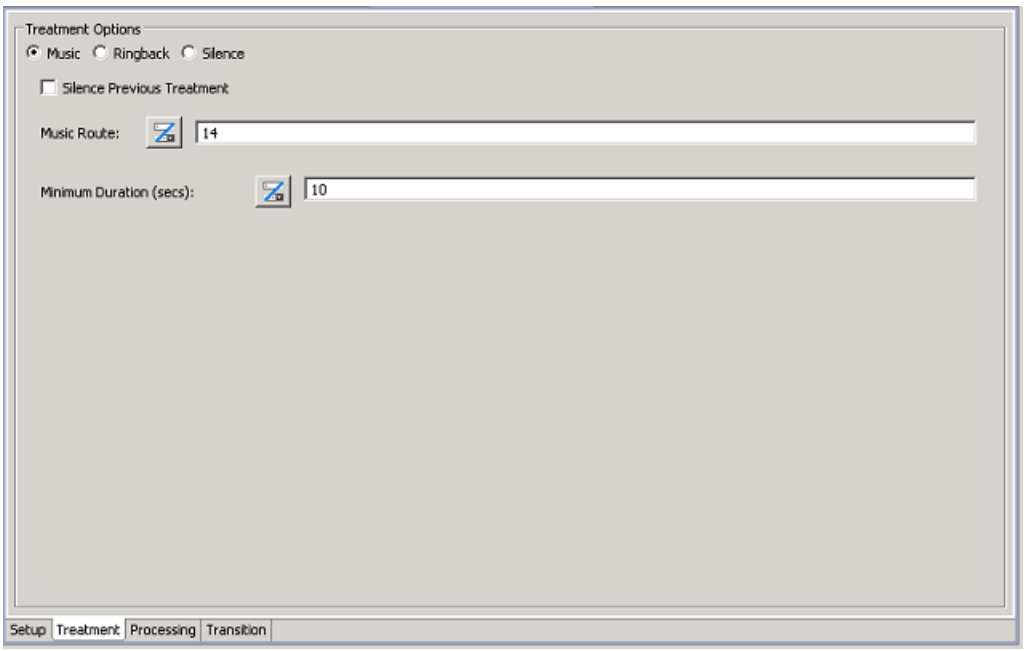
Procedure

1. In Orchestration Designer, with your flow application open, double-click the treatment block icon.
2. Click the **Setup** tab to configure the general details for the block. Configure PlayPop as the name of this treatment block.
3. Click the **Treatment** tab.
4. Select **Music**.
5. In the **Route Music** box, type the route number for the music of your choice.
6. Select the Main [MyApplication] flow application view.
7. Left-click the PlayCollectedDigits block and then right-click on the PlayPop treatment block, and select **(Dis)Connect**. This connects the output of the PlayCollectedDigits block with the input of the PlayPop block.

Example

For example, create a Treatment block to play music for 10 seconds. The Music Route number must match a route number configured in Contact Center Manager Administration.

Example of a Treatment block to play music:



Creating a Queue to Skillset block

About this task

Using Orchestration Designer (OD), create a Queue to Skillset block to route customer calls to an appropriate skillset.

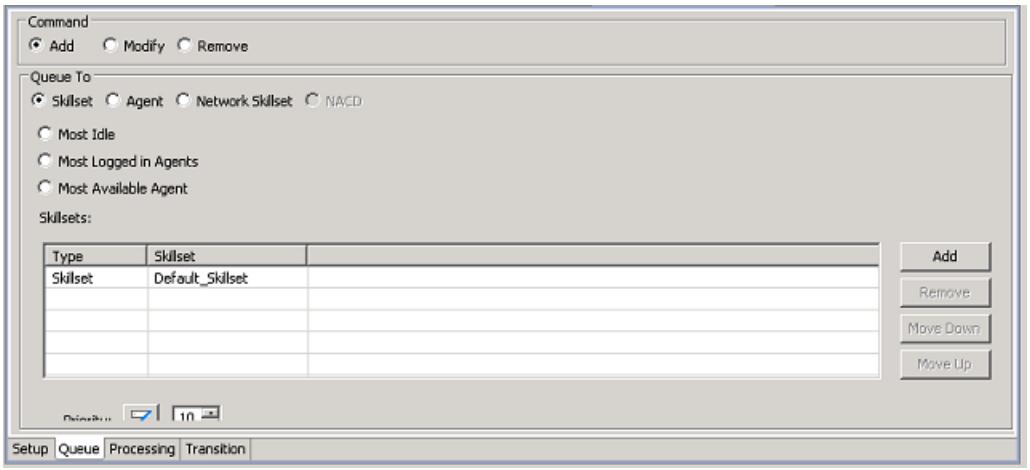
Procedure

1. In Orchestration Designer, with your flow application open, double-click the Queue to Skillset block icon.
2. Click the **Setup** tab to configure the general details for the block. Configure QueueToSkillset as the name of this Queue to skillset block.
3. Click the **Queue** tab.
4. Under **Command**, select **Add**, to add the contact to the queue in the flow application.
5. Under **Queue To**, select **Skillset**.
6. Beside the **Skillsets** table, click **Add**.
7. Expand **Application Variables**> **SKILLSET**, and select **Default_Skillset**.
8. Click **OK**.
9. Beside **Priority**, use the scroll buttons to assign a priority to the contact.

10. Select the Main [MyApplication] flow application view.
11. Left-click the PlayPop treatment block and then right-click on the QueueToSkillset block, and select **(Dis)Connect**. This connects the output of the PlayPop treatment block with the input of the QueueToSkillset block.
12. Left-click the QueueToSkillset block and then right-click on the **Exit** block, and select **(Dis)Connect**. This connects the output of the QueueToSkillset block with the **Exit** block, ending the flow application.
13. Click **X** on the Queue block to close it.
14. Click **File** > **Save**.
15. If you receive a confirmation box, click **OK**.

Example

For example, create a Queue to Skillset block to route customer calls to the default skillset:



Configuring the Flow Application Contact Router

About this task

Configure the Orchestration Designer contact router for incoming contacts. Contact routes are assigned based on CDN (route point) or the DNIS number of a contact. For each CDN (route point) or DNIS number, you can designate an application that controls contact handling.

Associate a CDN (route point) to your Flow Application, to ensure that calls to the CDN (route point) are treated by your application.

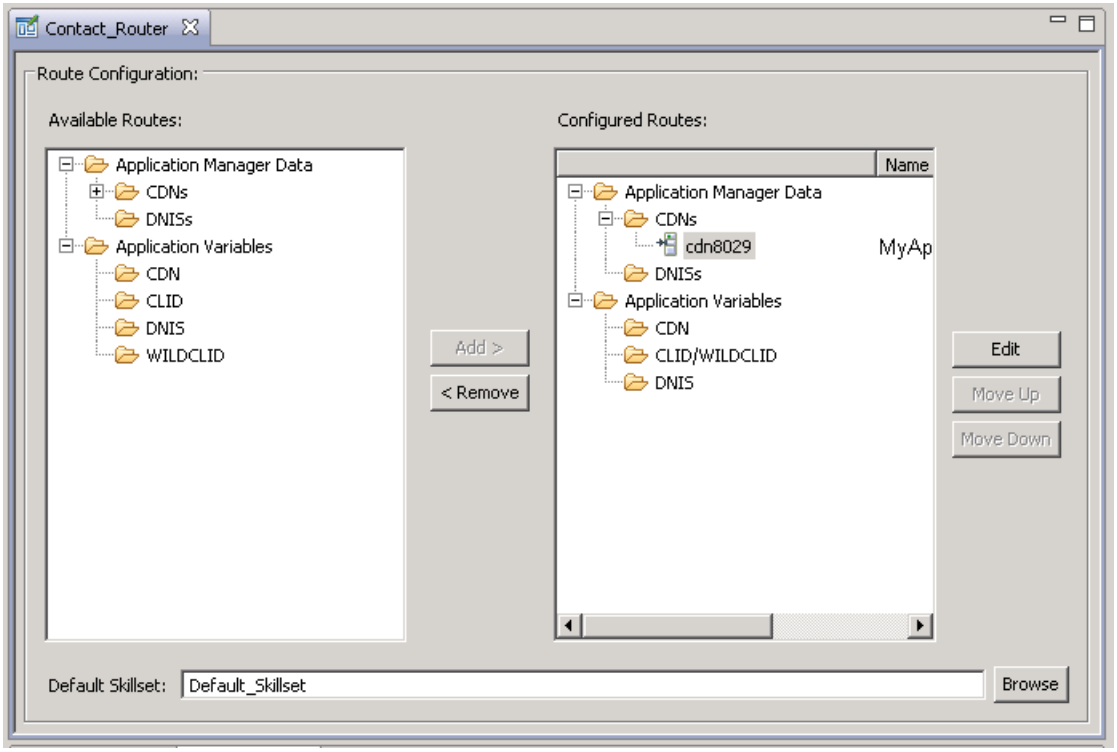
Procedure

1. Open Orchestration Designer.
2. Open the **Applications** folder.
3. Right-click on the **Master_Script**.
4. Select **Open**. The Contact_Router pane appears.
5. In the **Route Configuration** editor, under **Available Routes**, select the required CDNs from the **CDNs** list.
6. Click **Add >**.
7. On the Application Chooser dialog box, select the application to process this CDN, and click **OK**.
8. To position the application, click **Move Up** or **Move Down**.
9. To change the application, click **Edit**.
10. Under **Available Routes**, select the required DNISs from the **DNISs** list.
11. Click **Add >**.
12. From the **Default Skillset** list, click **Browse** and select the skillset.
13. Click **File** > **Save**.

Example

For example, associate a CDN (route point) with your Flow Application. Call to the CDN (route point) are then treated by your application.

Example of configuring Orchestration Designer Contact Router:


Contact_Router
Route Configuration:
Available Routes:
Application Manager Data
CDNs
DNISs
Application Variables
CDN
CLID
DNIS
WILDCLID
Add >
< Remove
Configured Routes:
Name
Application Manager Data
CDNs
cdn8029
MyAp
DNISs
Application Variables
CDN
CLID/WILDCLID
DNIS
Edit
Move Up
Move Down
Default Skillset:
Default_Skillset
Browse

Chapter 10: Contact Center Manager Administration commissioning

Commission Contact Center Manager Administration (CCMA) after you install Contact Center Manager Administration server software to prepare your server for Avaya Aura® Contact Center operations.

Contact Center Manager Administration security access allows a user with full access to configure your Contact Center. 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. For more information about the Security Framework configuration, see Security Framework commissioning on page 185.

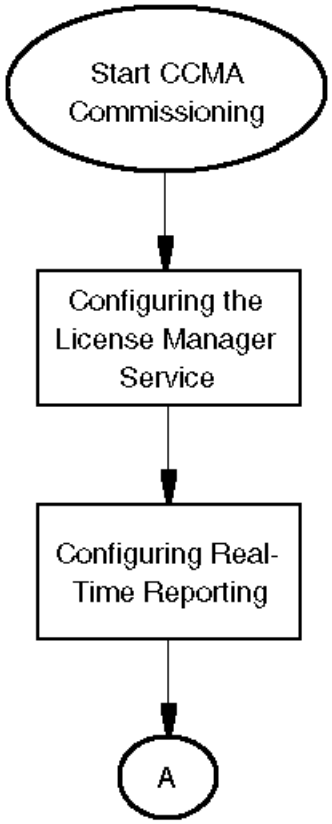
Prerequisites for Contact Center Manager Administration commissioning

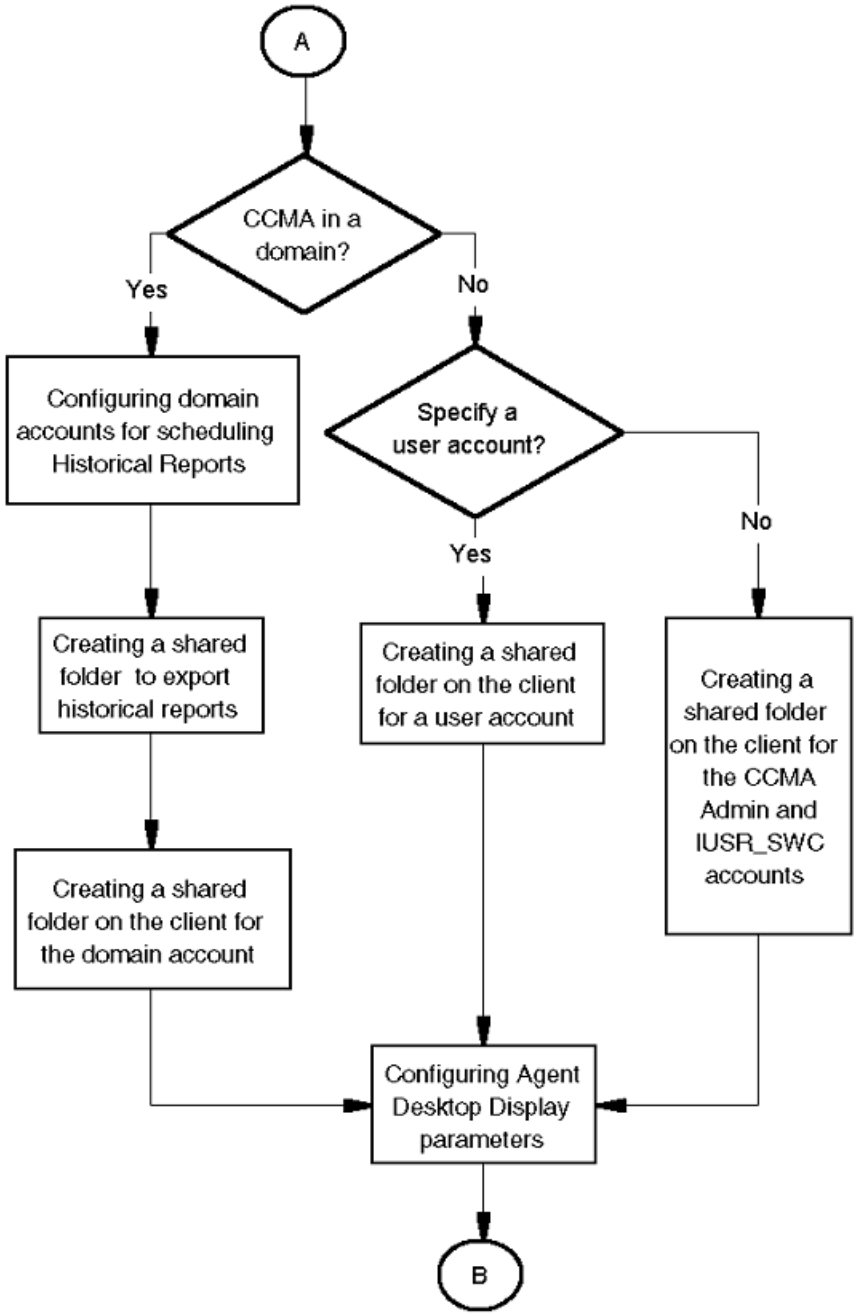
- Install the Contact Center Manager Administration software.
- Read *Avaya Aura® Contact Center Fundamentals* (NN44400-110).
- Ensure that you have administrator privileges on the server on which you installed the Contact Center Manager Administration server software.

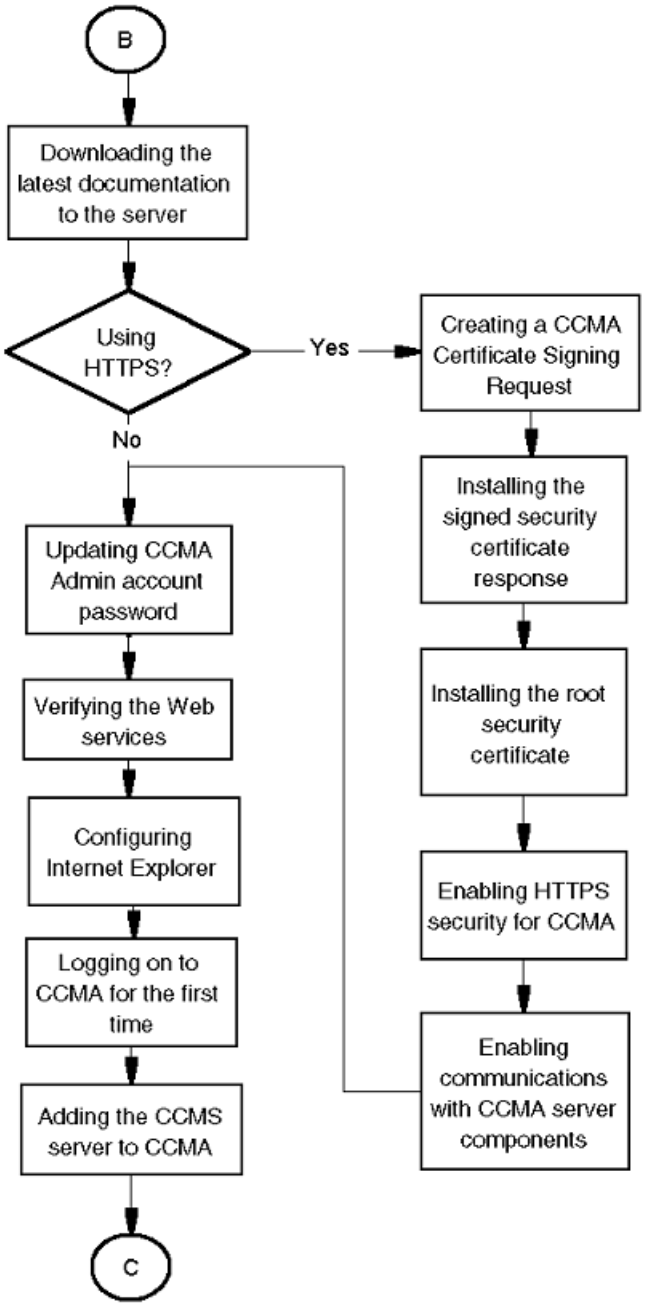
Contact Center Manager Administration commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to commission Contact Center Manager Administration.


Start CCMA Commissioning
Configuring the License Manager Service
Configuring Real-Time Reporting
A


A
CCMA in a domain?
Yes
No
Configuring domain accounts for scheduling Historical Reports
Specify a user account?
Yes
No
Creating a shared folder to export historical reports
Creating a shared folder on the client for a user account
Creating a shared folder on the client for the CCMA Admin and IUSR_SWC accounts
Creating a shared folder on the client for the domain account
Configuring Agent Desktop Display parameters
B


B
Downloading the latest documentation to the server
Using HTTPS?
Yes
Creating a CCMA Certificate Signing Request
No
Installing the signed security certificate response
Updating CCMA Admin account password
Installing the root security certificate
Verifying the Web services
Enabling HTTPS security for CCMA
Configuring Internet Explorer
Logging on to CCMA for the first time
Enabling communications with CCMA server components
Adding the CCMS server to CCMA
C

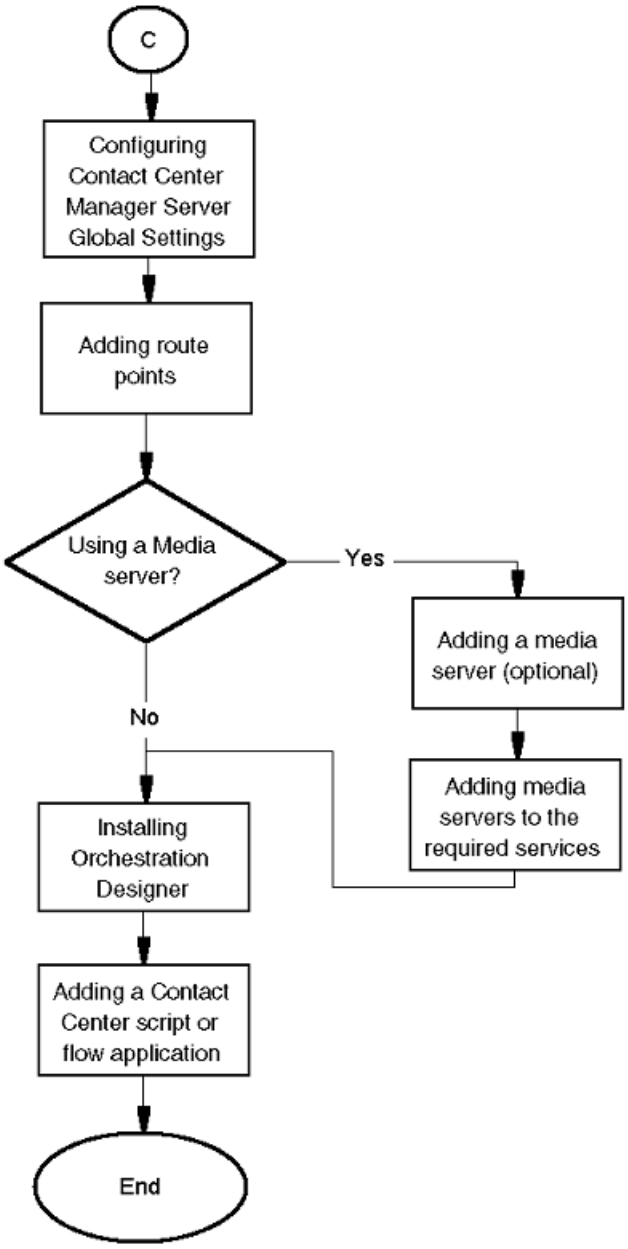


Figure 20: Contact Center Manager Administration commissioning procedures

Job aid: Timing

The estimated time to commission Contact Center Manager Administration is 1 hour.

Configuring the License Manager Service

Before you begin

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

About this task

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

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

Procedure

1. Log on to the Contact Center Manager Administration server as an administrator.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Configuration**.
3. In the left pane, expand **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 License Manager server.
6. In the **Primary Server's Port** box, type port number for the primary License Manager server.
7. If you have a standby License Manager server, in the **Standby Server's IP Address** boxes, type the IP address for the standby License Manager server.
8. If you have a standby License Manager server, in the **Standby Server's Port** box, type the port number for the standby License Manager server.
9. Click **OK** to submit the information.
10. In the **Configuration Completed** dialog box, click **OK**.
    A dialog box appears and prompts you to restart the License Manager Service.
11. Click **Yes**.
12. Click **OK**.

13. Close all windows.

Configuring Real-Time Reporting

Before you begin

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

About this task

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

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

Procedure

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

Important:

You can adjust the default values; however, reducing the Output Rate value and the Transform Rate value increases the workload on the Contact Center Manager Administration server.

8. For the **OAM Timeout** box, accept the default value (10 000).
9. Select the **Compress Realtime Data Packets** check box.

   Important:

   If you clear this check box, you disable real-time data packet compression.
10. In the **Transmission Options** area, select one of the following options:
    - If your network supports multicast traffic, select **Multicast**. Avaya recommends this option.
    - To support both transmission types, select **Multicast and Unicast**.
11. If you selected the **Multicast** option, proceed to step 14 on page 128.
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 restarting, and closes after the service successfully restarts.
15. Close all windows to complete the procedure.

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 data 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 you view a report using the Historical Reporting component.

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

Configuring domain accounts to allow scheduling Historical Reports to a Network Server

Before you begin

- Understand how to update the CCMA Admin user password; see Updating the CCMA Administration user password on page 144.

About this task

If Contact Center Manager Administration is on a domain, configure domain accounts to allow Historical Reports to run and be saved on a network server.

Procedure

1. Run the iceAdminPasswordChange utility.
2. Click the **Domain Account** icon.
3. Update the Domain Name, Domain User and Password.
4. Click **OK**.

Creating a shared folder to export historical reports

Before you begin

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

About this task

Create a shared folder to export historical reports if you want multiple users to access scheduled historical reports stored in this folder from other computers.

Procedure

1. Log on to the server on which you installed the Contact Center Manager Administration server software.
2. Create a folder. Name the folder **Exported Reports**.
3. Right-click the new folder and select **Properties**.
4. In the **Properties** dialog box, on the **Sharing** page, click **Advanced Sharing**.
5. Select **Share this folder**.

6. Click **Permissions**.
7. Click **Add**.
8. In the **Select Users or Groups** dialog box, click **Advanced**.
9. Click **Find Now**.
10. In the expanded portion of the **Select Users or Groups** dialog box, locate and select the **iceAdmin** account (this is the CCMA Admin account).

    OR

    Select the domain account used for IIS directory security.
11. Click **OK**.
12. In the **Select Users or Groups** dialog box, click **OK**.
13. In the **Permissions** dialog box, select the account that you selected in step 10 on page 130.
14. Select the **Allow** check box for the following:
    - **Change**
    - **Read**
15. Click **Apply**.
16. Click **OK** to close the **Permissions for Exported Reports** dialog box.
17. Click **OK** to close the **Advanced Sharing** dialog box.
18. Click **OK** to close the **Exported Reports Properties** dialog box.

Creating a shared folder on the client with read permissions for the domain

Before you begin

- Ensure that Contact Center Manager Administration is part of a network domain.
- Configure the domain account. See Configuring domain accounts to allow scheduling Historical Reports to a Network Server on page 129.

About this task

Create a shared folder with read permissions on the client for the domain account if Contact Center Manager Administration is part of a network domain. Use the shared folder to synchronize historical reports.

Procedure

1. On the client, create a folder.
2. Right-click the shared folder, and select **Properties**.
3. In the **New folder Properties** dialog box, click the **Sharing** tab.
4. Click **Advanced Sharing**.
5. Click **Share this folder**.
6. Click **Permissions**.
7. In the **Permissions for New folder** dialog box, Select **Everyone**.
8. Click **Remove** to remove the Everyone account.
9. Click **Add**.
10. In the **Select Users 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 domain or directory security user account used to join the Contact Center Manager Administration server to the network domain.
13. Click **OK**.
14. In the **Select Users or Groups** dialog box, click **OK**.
15. In the **Permissions for New folder** dialog box, select the newly added group or user name account.
16. Select the **Allow** check box for **Read**.
17. Click **OK**.
18. Click **OK**.
19. Click **OK** to save your changes and close the **New folder Properties** dialog box.

Creating a shared folder on the client with read permissions for a user

Before you begin

- If Contact Center Manager Administration is part of a domain, configure the domain account. See Configuring domain accounts to allow scheduling Historical Reports to a Network Server on page 129.

About this task

Create a shared folder with read permissions on the client for a user account to ensure that the user can access the folder on the client.

Procedure

1. On the client, create a folder.
2. Right-click the folder, and select **Properties**.
3. In the **New folder Properties** dialog box, click the **Sharing** tab.
4. Click **Advanced Sharing**.
5. Click **Share this folder**.
6. Click **Permissions**.
7. In the **Permissions for New folder** dialog box, select the user login name.
8. Select the **Allow** check box for **Read**.
9. Clear all other check boxes.
10. Click **Apply**.
11. Click **OK**.
12. Click **OK**.
13. In the **New folder Properties** dialog box, click **Close**.

Creating a shared folder on the client PC with read permissions for the IUSR_SWC and CCMA Admin accounts

Before you begin

- Ensure that Contact Center Manager Administration is part of a workgroup.

About this task

If Contact Center Manager Administration is part of a workgroup, create a shared folder on the client PC with Read permissions for the IUSR_SWC and CCMA Admin accounts.

If you choose this option, you must maintain two additional accounts on the client PC. Security issues can arise because the Contact Center Manager Administration server uses these accounts to run the Web site.

Procedure

1. On the client, create a folder.
2. Right-click the folder, and select **Properties**.
3. In the **New folder Properties** dialog box, click the **Sharing** tab.
4. Click **Advanced Sharing**.
5. Click **Share this folder**.
6. Click **Permissions**.
7. In the **Permissions for New folder** dialog box, Select **Everyone**.
8. Click **Remove** to remove the Everyone account.
9. Click **Add**.
10. In the **Select Users 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 **IUSR_SWC** user account.
13. Click **OK**.
14. In the **Select Users or Groups** dialog box, click **OK**.
15. In the **Permissions** dialog box, select **IUSR_SWC**.
16. Select the **Allow** check box for **Read**.
17. Click **Apply**.

18. Perform step 9 on page 133 to step 17 on page 133 to add read permissions for the iceAdmin user account (the CCMA Admin account).
19. Click **OK**.
20. Click **OK** to close the **Advanced Sharing** dialog box.
21. Click **Close** to close the **New folder Properties** dialog box.

Configuring Agent Desktop Display parameters on the server

Before you begin

- Ensure that you have administrative privileges on the server on which you installed the Contact Center Manager Administration server software.

About this task

Configure parameters on the Contact Center Manager Administration server to use Agent Desktop Display on a client.

Procedure

1. Log on to the server on which you installed the Contact Center Manager Administration server software.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Agent Desktop Displays** > **Server Configuration Parameters**.
3. In the **Configuration Parameters** dialog box, in the **IP multicast address** box, confirm that the address is the Contact Center Manager Administration server IP send address that you configured in the RTR Configuration Tool.
4. In the **Refresh rate (seconds)** box, type the rate in seconds at which you want the real-time data in the displays to be refreshed.
5. 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.
6. From the **View mode** list, select the mode in which you want to view the collected data:
    - **Moving window**
    - **Interval-to-date**
7. 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.

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.

8. To disable automatic notifications for Agent Desktop Display client upgrades, select the **Disable Automatic ADD Client Upgrade** check box .

   If you select this check box, agents receive no prompts to download available Agent Desktop Display client upgrades.

9. In the **Statistics Configuration** table, choose the statistics to appear in the Agent Desktop Display. You can add statistics columns to the displays or remove columns that you no longer want to show.
10. To add the statistics column to the displays, select the **Show** check box for each statistic.
11. Use the column order buttons to arrange the order in which the statistics columns appear. Select the statistic to move, and then click the up or down button to change its position.

    The statistic that you place at the top of the Statistics Configuration table appears in the first column of the display.

12. To assign the threshold display color, select a statistic.
13. From the following lists, select the threshold color for the highlighted statistic:

    - **Less than Level 1**
    - **Between Level 1 and Level 2**
    - **Greater than Level 2**

    If you configure no threshold levels in the Configuration component of Contact Center Manager Administration or in Contact Center Manager Server, the values appear in white in the Agent Desktop Display.

14. Repeat step 12 on page 135 to step 13 on page 135 for each statistic for which you want to configure threshold display colors.
15. If you want the selected statistic to blink in the Agent Desktop Display when its value reaches the threshold, select the **Blink** check box.
16. If you want the Agent Desktop Display to beep when the threshold value reaches the threshold, select the **Beep** check box.
17. If you did not select the **Beep** check box, proceed to step 20 on page 135.
18. To indicate that a beep occurs only once, select **Once**.
19. To indicate that a beep occurs continuously until the statistic reaches an acceptable value, select **Continuously**.
20. Click **Save**.

Variable definitions

Name	Description
IP multicast address	The IP multicast addresses that you select for RSM sending and receiving must be 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.
Max agents	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 1000 agents. The maximum value that you can type in this box is 3000 agents. For information about performance and sizing requirements for Contact Center Manager Administration, see the *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
Refresh rate	The minimum value that you can type in this box is 2 seconds. You must specify a value for the refresh rate.
View mode	Select one of the following view modes: • Moving window—In moving window mode, statistics 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.

Downloading the latest documentation to the CCMA server

Before you begin

- Download Adobe Acrobat Reader on the client to open the documents from the Contact Center Manager Administration server.

About this task

Download the documentation related to the Contact Center Manager Administration server to make it available directly through the Help menu. You must copy the guides to the Documentation folder on the Contact Center Manager Administration server.

Because customer documentation is updated on a regular basis, you must download the latest versions of the documentation from the support site to the Documentation folder regularly to ensure that you have the most up-to-date information.

Procedure

1. Browse to www.avaya.com/support.
2. In the left pane, click **Products**.
3. Type Avaya Aura® Contact Center in the **Please enter the name of your product** box.
4. On the Avaya Aura® Contact Center page, in the left pane, click **Documentation**.
5. Click **View All Documents**.
6. Copy the following documents to the Contact Center Manager Administration server:
    - *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611)
    - *Avaya Aura® Contact Center Fundamentals* (NN44400-110)
    - *Avaya Aura® Contact Center Performance Management* (NN44400-710)
    - *Avaya Aura® Contact Center Performance Management Data Dictionary* (NN44400-117)
    - *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (NN44400-510)
7. Rename the document PDF files to match the following, respectively:
    - Contact Center Manager Administration-Client Administration.pdf
    - Contact Center Fundamentals.pdf
    - Contact Center Performance Management.pdf
    - Contact Center Performance Management Data Dictionary.pdf

- Contact Center Configuration-Orchestration Designer Application Development.pdf

8. Move the documents to the document folder on the Contact Center Manager Administration server:

   <INSTALLDIR>\Avaya\Contact Center\Manager Administration\Apps\documentation\guides

   Important:

   The downloaded documents replace existing documents in the document folder.

Variable definitions

Name	Description
<INSTALLDIR>	The Contact Center Manager Administration installation drive. The installer chooses the location during installation.

Creating a CCMA Certificate Signing Request

About this task

On the Contact Center Manager Administration server, use the Internet Information Services (IIS) Manager to generate a security Certificate Signing Request (CSR). You can then sign the security Certificate Signing Request (CSR) using Security Framework or a third-party Certificate Authority.

For more information about using a Certificate Authority server to sign security certificates, see Certificate Authority commissioning on page 159.

For more information about using Security Framework to sign security certificates, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Click **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
3. Select the server node from the tree view.
4. In the right hand list view, double-click **Server Certificates**.

5. In the **Actions** pane on the right, select **Create Certificate Request**.
6. On the **Request Certificate** wizard, on the Distinguished Name Properties window, enter the Distinguished Name Property values.
7. Click **Next**.
8. On the **Cryptographic Service Provider Properties** window, select the default values.
9. Click **Next**.
10. On the **File name** window, enter a name and location for the Certificate Signing Request. Avaya recommends that you use a descriptive name for the Certificate Signing Request text file.
11. Click **Finish**.
12. Use a Certificate Authority or Security Framework server to sign the Certificate Signing Request text file.

Variable definitions

Name	Description
Common name	The fully-qualified domain name (FQDN) for the certificate.
Organization	The name of the organization that uses the certificate.
Organizational unit	The name of the department or division in the organization that uses the certificate.
City/locality	The un-abbreviated name of the city or locality where your organization or organizational unit is located.
State/province	The un-abbreviated name of the state or province where your organization or organizational unit is located.
Country/region	The name of the country or region where your organization or organizational unit is located.

Installing the Signed Security Certificate Response

Before you begin

- On the CCMA server, use the Internet Information Services (IIS) Manager to generate a security Certificate Signing Request (CSR).
- Using Security Framework or a third-party Certificate Authority, sign the security Certificate Signing Request (CSR).
- Copy the signed certificate to the CCMA server.

About this task

Install the Security Framework or a third-party Certificate Authority signed certificate using the Internet Information Services (IIS) Manager on the Contact Center Manager Administration server.

The default Security Framework signed certificate is ClientCertificate.CER.

For more information about using a Certificate Authority server to sign security certificates, see Certificate Authority commissioning on page 159.

For more information about using Security Framework to sign security certificates, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Click **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
3. In the left hand pane, select the server node from the tree view.
4. In the right hand list pane, double-click **Server Certificates**.
5. From the **Actions** pane, select **Complete Certificate Request**.
6. In the Complete Certificate Request window, browse to and select the signed Certificate Response (.CER) file received from the Certificate Authority or Security Framework server.
7. Click **Open**.
8. On the Specify Certificate Authority Response window, in the **Friendly name** box, enter a friendly name for the certificate.
9. Click **OK**.

Installing the Root Security Certificate

Before you begin

- On the CCMA server, use the Internet Information Services (IIS) Manager to generate a security Certificate Signing Request (CSR).
- Using Security Framework or a third-party Certificate Authority, sign the security Certificate Signing Request (CSR).
- Copy the root security certificate to the CCMA server.

About this task

Install the Security Framework or a third-party Certificate Authority Root Certificate using the Microsoft security Certificates console on the Contact Center Manager Administration server.

Add the Security Framework or third-party Certificate Authority Root Certificate as both an Intermediate Certificate and as a Trusted Root Certificate.

The default Security Framework root certificate is RootCACertificate.CER.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Click **Start**, **Run**.
3. Type `mmc`, and then click **OK**.
   The Microsoft Management Console (Console) window opens.
4. In the Console window, click **File** and select **Add/Remove Snap-in**.
5. From the Add or Remove Snap-ins window, select **Certificates**.
6. Click **Add**.
7. Select **Computer Account**, and then click **Next**.
8. Select **Local Computer**, and then click **Finish**.
9. Click **OK**.
10. In the Console window, expand the **Certificates** folder on the left.
11. Right-click **Intermediate Certification Authorities**, and select **All Tasks**.
12. Click **Import**.
13. In the **Certificate Import** wizard, click **Next**.
14. Click **Browse** to find the root certificate file, for example RootCACertificate.CER.
15. Click **Next**.

16. Select **Place all certificates in the following store**.
17. Click **Browse**, and select **Intermediate Certification Authorities**.
18. Click **Next**.
19. Click **Finish**.
20. In the Console window, expand the **Certificates** folder on the left.
21. Right-click **Trusted Root Certification Authorities**, and select **All Tasks**.
22. Click **Import**.
23. In the **Certificate Import** wizard, click **Next**.
24. Click **Browse** to find the root certificate file, for example RootCACertificate.CER.
25. Click **Next**.
26. Select **Place all certificates in the following store**.
27. Click **Browse**, and select **Trusted Root Certification Authorities**.
28. Click **Next**.
29. Click **Finish**.

Enabling HTTPS security for CCMA

About this task

Enable HTTPS and Secure Sockets Layer (SSL) for the CCMA web site. Configure HTTPS, SSL port number, and enforce SSL security for the CCMA Web site.

Procedure

1. Click **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.
2. On the tree view under the server node, from the list of **Sites**, select the **Default Web Site**.
3. On the **Actions** pane on the right, select **Bindings**.
4. On the Site Bindings window, click **Add**.
5. In the Add Site Binding window, from the **Type** list, select **https**.
6. In the **Port** box, type the SSL port number. The default port is 443.
7. From the **SSL Certificate** list, select the installed signed certificate, using the certificate friendly name.
8. Select **OK**.

9. Select **Close**.
10. On the tree view under the server node, from the list of **Sites**, select the **Default Web Site**.
11. On the center list view, double-click **SSL Settings**.
12. Select **Require SSL**.
13. Select **Ignore**.
14. On the **Actions** pane, select **Apply**.

Enabling communications with CCMA server components

About this task

Enable secure communications with CCMA server components such as Orchestration Designer and Open Interfaces Web Services.

Use the Contact Center “wcApplyChanges” utility to configure Orchestration Designer and Open Interfaces Web Services to work when CCMA uses HTTPS security.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Click **Start** > **Run**.
3. In the **Open** box, enter `cmd`.
4. At the command prompt, enter `wcApplyChanges -i`.

Procedure job aid

Example of using the CCMA wcApplyChanges utility.

```
Command Executed...wcApplyChanges.exe -i
C:\Users\Administrator>wcapplychanges -i
Entering...
Command Executed...wcApplyChanges.exe -i
Checking IIS - Is SSL Port populated? answer: True
Successful update: web.config.SSL used
Exiting!
```

Updating the CCMA Administration user password

Before you begin

- Use System Control and Monitor Utility (SCMU) to stop all Contact Center Manager Administration services.
- Reset Internet Information Services (IIS) (using the **`iisreset`** command) on the Contact Center Manager Administration server.

About this task

Update the CCMA Administration account password on your Contact Center Manager Administration server using the iceAdmin Password Change utility.

The CCMA Administration account is an administrator account for the Contact Center Manager Administration server.

Procedure

1. Log on the server on which you installed the Contact Center Manager Administration server software.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Configuration**.
3. In the Avaya Applications Configuration window, in the left pane, expand **Avaya** > **Applications** > **iceAdmin Password Change**.
4. In the right pane, click the **iceAdmin Password Change** icon.
5. In the **Old Password** box, type the current password for the CCMA Admin user account.

   Important:

   If you use this utility for the first time, you cannot enter the old password because the box is dimmed.
6. In the **New Password** box, type the new password for the CCMA Admin user account.
7. In the **Confirm Password** box, type the new password again.
8. Click **OK**.
9. Use System Control and Monitor Utility (SCMU) to start Contact Center Manager Administration.

Verifying the Web Services

About this task

Test the Web Services to ensure CCMA web services are running correctly.

Procedure

1. Start Internet Explorer.
2. Enter the following: `http://<ccmaservername>/supportutil/testwebservices.asp`.

   The web services that appear in green are running correctly.

Configuring Internet Explorer

About this task

Configure Internet Explorer to access Contact Center Manager Administration.

Install Microsoft Internet Explorer 7.0 or later (32 bit version only). Contact Center Manager Administration supports only the 32 bit version of Microsoft Internet Explorer.

If you are using Security Framework on your client, ensure that the Security Framework server is also added as a trusted site in Internet Explorer.

Procedure

1. Start Internet Explorer.
2. From the menu, select **Tools** > **Internet Options**.
3. In the **Internet Options** dialog box, click the **Security** tab.
4. Click the **Trusted Sites** icon.
5. Click **Custom Level**.
6. In the **Security Settings** dialog box for trusted sites, under the **.NET Framework-reliant components** heading, select **Enable** for the following:
   - **Run components not signed with Authenticode**
   - **Run components signed with Authenticode**
7. Under the **ActiveX controls and plug-ins** heading, select **Enable** for the following:
   - **Automatic prompting for ActiveX controls**

- **Run ActiveX Controls and plug-ins**
- **Script ActiveX Controls marked safe for scripting**

8. Under the **Downloads** heading, select **Enable** for the following:
   - **Automatic prompting for file downloads**
   - **File download**
9. Under the **Miscellaneous** heading, for **Allow script-initiated windows without size or position constraints**, select **Enable**.
10. Under the **Miscellaneous** heading, for **Allow websites to open windows without address or status bars**, select **Enable**. (Applies to Internet Explorer 7.0 and later.)
11. Click **OK**.
12. If you enabled ActiveX options, when a message appears asking you to confirm your choice, click **Yes**.
13. Click the **Trusted Sites** icon.
14. Click **Sites**.
15. In the **Trusted sites** dialog box, clear the **Require server verification {https:} for all sites in this zone** check box.
16. In the **Add this Web site to the zone** box, type the server name (not the IP address) for your Contact Center Manager Administration server.

    OR

    If you used the fully qualified domain name when you installed Contact Center Manager Administration on the Contact Center Manager Administration server, in the **Add this Web site to the zone** box, type the fully qualified domain name.
17. Click **Add**.
18. In the **Add this Web site to the zone** box, type the server name (not the IP address) for your Contact Center Multimedia server.
19. Click **Add**.
20. If your contact center includes a Predictive Reporting server, in the **Add this Web site to the zone** box, type the server name (not the IP address) for your Predictive Reporting server.
21. Click Add.
22. Click **Close** to return to the **Internet Options** dialog box.
23. Click the **Privacy** tab.
24. In the **Pop-up Blocker** section, select the **Block pop-ups** check box.
25. Click **Settings**.

26. In the **Pop-up Blocker Settings** dialog box, in the **Address of website to allow** box, type the Contact Center Manager Administration URL, http://<server name>/.
27. Click **Add**.
28. Click **Close**.
29. In the **Internet Options** dialog box, click the **Advanced** tab.
30. Under **Browsing**, clear the **Reuse windows for launching shortcuts** check box.
31. If HTTPS and SSL are enabled, and if you are using Internet Explorer 9.0, under **Security** clear the **Do not save encrypted pages to disk** check box.
32. Click **OK** to exit the **Internet Options** dialog box.
33. Restart Internet Explorer to activate your changes.

Logging on to Contact Center Manager Administration for the first time

Before you begin

- Configure Internet Explorer.
- Ensure that the Contact Center Manager Server name is registered with either the Domain Name Service (DNS) or the HOSTS table.

About this task

When you log on to Contact Center Manager Administration for the first time, you must log on as the default administrator, webadmin. For security reasons, Avaya highly recommends that you change the default password when you first log on to the application. Contact Center Manager Administration user passwords can contain only English characters and special characters.

If you are using HTTPS and SSL with CCMA, Avaya recommends that you follow your organization's security policies and procedures. You may need to install the Certificate Authority root certificate on each CCMA Web client computer.

Procedure

1. Start Internet Explorer.
2. In the **Address** box, type the server name. For example, http://<server name>. OR, if CCMA is using HTTPS enter; https://<server name>.

Important:

You must log on using the Contact Center Manager Administration server name instead of the IP address.

3. Press **Enter**.
4. In the Contact Center Manager Administration main logon window, click **Change Password**.
5. In the **Change Password** dialog box, in the **User name** box, type the default user name. For information about default login values, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).
6. In the **Old password** box, type the default password.
7. In the **New password** box, type a new password.

   Contact Center Manager Administration user passwords can contain English characters and special characters only.
8. In the **Confirm password** box, type the new password again.

   You can modify the default password only. You cannot change the default user name, webadmin.

   Important:

   If you lose or forget the new webadmin password, you cannot log on to Contact Center Manager Administration as the webadmin administrator. To avoid this scenario, in Access and Partition Management, you can create a new user account with administrator rights, such as tempadmin. If you forget or lose the new webadmin password, you can log on to the Contact Center Manager Administration server as tempadmin to change the password. If you forget all passwords for accounts with administrator rights, please contact support to have the webadmin password reset.
9. Click **Submit**.
10. In the main logon window, in the **User ID** box, type the user name.
11. In the **Password** box, type the new password.
12. Click **Login**.
13. Click **OK**.
14. In the **Server Name** box, type the computer name of the Contact Center Manager Server. Do not enter the fully qualified domain name.
15. Press **Tab**.
    The server IP address automatically appears in the IP Address box.
16. In the **Display Name** box, type the name of the Contact Center Manager Server as you want it to appear in the system tree in Contact Center Manager Administration.

Important:

You must use the server name, not the server IP address, because using an IP address causes errors in Real-Time Reporting functionality. The system automatically assigns a display name that is the same as the server name. If you enter a different display name, the name must be unique.

17. In the **Login ID** box, type the sysadmin user name.
18. In the **Password** box, type the password for the Contact Center Manager Server. For information about default login values, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).
19. If you receive a logon sequence error message, log on to Server Utility to check your user name and password.
20. Click **Submit**.
    The Contact Center Manager Administration launchpad appears.

Variable definitions

Name	Description
Contact Center Manager Administration Server name	The name of the Contact Center Manager Administration server.

Adding the Contact Center Manager Server to Contact Center Manager Administration

About this task

Add the Contact Center Manager Server to Contact Center Manager Administration to enable contact center configuration.

Procedure

1. Log on to Contact Center Manager Administration with administrative privileges.
2. On the **Launchpad**, click **Configuration**.
3. From the menu, choose **Server** > **Add Server**.
4. From the **Type** list, select **CCMS**.

5. In the **Server Name** box, type the computer name of the Contact Center Manager Server.
6. Press **Tab**.
   The Contact Center Manager Server IP automatically appears in the IP Address box.
7. In the **Display Name** box, type the name of the Contact Center Manager Server as you want it to appear in the system tree of Contact Center Administration.

   The system automatically assigns a display name that is the same as the server name. To enter a different display name, you must enter a unique name.
8. In the **Login ID** box, type the Login ID for the Contact Center Manager Server. The Login ID corresponds to a user account created using the Contact Center Manager Server Utility.
9. In the **Password** box, type the password for the Contact Center Manager Server.
10. Click **Submit**.

Configuring Contact Center Manager Server Global Settings

About this task

Configure Contact Center Manager Server Global Settings to setup Agent Order Preference, Default DN, Expected Wait Time algorithm, and the server designated for historical statistical data.

Configure a Default DN to catch treated calls that are defaulted by the contact center script and to catch calls not answered by agents. Avaya recommends that you configure an attendant as the Default DN.

Procedure

1. Log on to Contact Center Manager Administration.
2. In the left pane, expand the Contact Center Manager Server on which to configure global settings.
3. Select the **Global Settings** folder.
4. Configure the global settings for your system based on the fields listed in the **Global Settings** window.
5. In the **Default DN** box, type the default DN to use when a script defaults or a treated call is not answered. Avaya recommends that you configure an attendant as the Default DN.

6. Click **Submit**.

Procedure job aid

Avaya recommends that you configure an attendant as the Default DN.

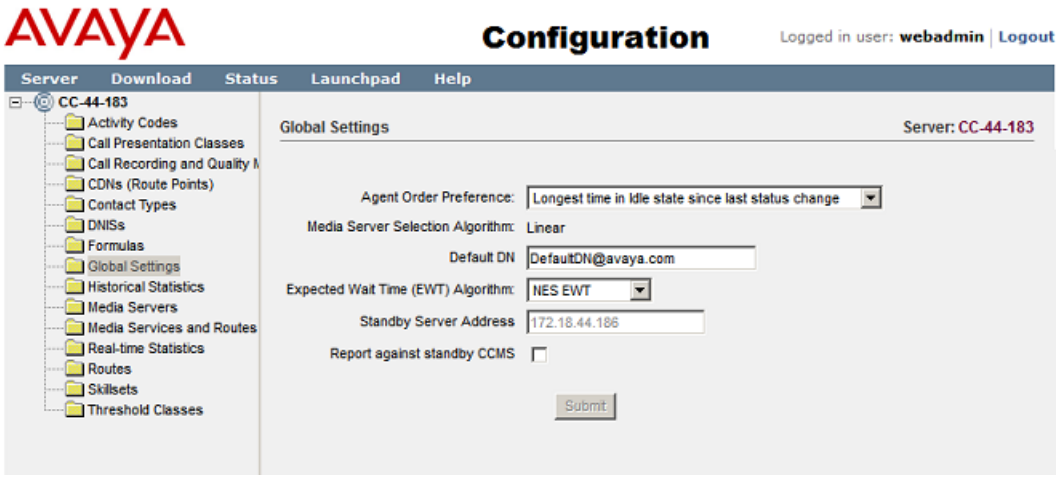


Figure 21: Example of configuring the Default DN

Adding route points

About this task

Add route points to your contact center to route contacts.

Procedure

1. Log on to Contact Center Manager Administration with administrative privileges.
2. On the **Launchpad**, click **Configuration**.
3. In the left pane, click the plus sign (+) next to the Contact Center Manager Server to which you want to add the route point.
4. Select the **CDNs (Route Points)** folder.
5. On the **CDNs (Route Points)** window, in the **Name** box, type the name of the route point.
6. In the **Number** box, type the number for the route point.
7. In the **URI** box, type the value for the Uniform Resource Indicator (URI) of the route point on the server.

8. From the **Call Type** list, select **Local**.
9. Select the **Acquired** check box.
10. Click any other row of the table to add and acquire the Route Point.

Variable definitions

Name	Description
Name	A name that describes the route point, type, or function (for example, IM_sales for an IM route point that handles sales).
Number	The number used internally by the SIP-enabled contact center that is inherited from AML-based contact centers and appears in the TFE scripts as a CDN.
URI	The URI the SIP-enabled contact center accepts for processing by the SIP-enabled contact center. INVITEs received that do not match these URI are rejected. Avaya recommends that you use lowercase letters for URIs.
Type	Local or network. You must enable the networking option to use the Route Point for network calls.
Acquired	Select this check box to indicate to the system to acquire and process calls using this URI.

Adding media servers

About this task

Add media servers to Contact Center Manager Server using Contact Center Manager Administration.

Avaya Aura® Contact Center uses Avaya Media Server media processing capabilities to support conferencing, announcements and dialogs. Each Avaya Media Server in a contact center is configured in Contact Center Manager Administration as a Media Server and assigned to handle conference, announcement or/and dialogs media services.

Note:

Media servers are used only in SIP-enabled contact centers. If you have an AML-based contact center, skip this procedure.

Procedure

1. Log on to Contact Center Manager Administration with administrator privileges.
2. On the **Launchpad**, click **Configuration**.
3. In the left pane, click the plus (+) sign next to the SIP-enabled Contact Center Manager Server.
4. From the list of configuration items for the Contact Center Manager Server, select **Media Servers**.
5. On the **Media Servers** window, in the **Server Name** box, type a name for the media server. If you are using the Avaya Media Server – High Availability (HA) feature, and if you have a pair of Avaya Media Server HA servers configured, type a name for the HA pair.
6. In the **IP Address** box, type the IP address of each Avaya Media Server media server. If you are using the Avaya Media Server – High Availability (HA) feature, and if you have a pair of Avaya Media Server HA servers configured, type the Managed IP address of the Avaya Media Server HA pair. On the Avaya Media Server the Managed IP address is configured under **High Availability** as the **Service IP Address**. For more information, see Enabling High Availability on the backup server on page 64.
7. In the **Port Number** box, type the port number.

   Important:

   The port number must match the Avaya Media Server port number. The default is 5060, but your Avaya Media Server can be set at 5070, for example, if Avaya Media Server is co-resident with CCMS.
8. Ensure that the value for **Transport** is **TCP** or **UDP**.
9. Click **Refresh Status**.
10. On the **Save Changes** message box, click **Yes**.
11. Repeat step 1 on page 153 to step 10 on page 153 for each media server to add.

Adding media servers to the required services

Before you begin

- Add the media servers to Contact Center Manager Server. See Adding media servers on page 152.

About this task

Each SIP-enabled contact center requires at least one Avaya Media Server to supply the following services:

- Announcements (ANNC)
- Conferences (CONF)
- Interactive Voice Response (IVR) dialog (DIALOG)

Avaya Aura® Contact Center uses Avaya Media Server media processing capabilities to support conferencing, announcements and dialogs. Each Avaya Media Server in a contact center is configured in Contact Center Manager Administration as a Media Server and assigned to handle conference, announcement or/and dialogs media services.

You must assign an Avaya Media Server media server for each announcement, conferencing and dialog service.

Note:

Media servers are used only in SIP-enabled contact centers. If you have an AML-based contact center, skip this procedure.

Procedure

1. Log on to Contact Center Manager Administration.
2. On the **Launchpad**, click **Configuration**.
3. In the left pane, click the plus sign (+) next to the SIP-enabled Contact Center Manager Server.
4. From the list of configuration items for the Contact Center Manager Server, select **Media Services and Routes**.
5. Ensure that each of the following Contact Center services is associated with at least one Avaya Media Server:
   - **ANNC**
   - **DIALOG**
   - **CONF**
6. Select **ANNC**.
7. Select the media server..

8. Select the arrow key.
9. Click **Submit**.
10. Repeat step 6 on page 154 to step 9 on page 155 for each service required.

Installing the Orchestration Designer client

About this task

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

Perform the following procedure to ensure that the version of the Orchestration Designer that you start from within the Contact Center Manager Administration application is current. You can also install the Orchestration Designer on any client to work with script or flow applications without affecting the Contact Center environment. For instructions to install the Orchestration Designer on a client, see *Avaya Aura® Contact Center Installation* (NN44400-311).

Procedure

1. Start Internet Explorer.
2. In the **Address** box, type the server name. For example, http://<Contact Center Manager Administration Server name>.
3. Press **Enter**.
4. Log on to the Contact Center Manager Administration browser using the configured password
5. On the **Launchpad**, click **Scripting**.
6. In the Scripting window, on the menu, click **Orchestration Designer**, and then click **Launch Orchestration Designer**.
7. In the message box requesting you to download a .msi file, click **OK**.
8. In the dialog box, click **Run**.
9. In the **Orchestration Designer- InstallShield Wizard**, click **Next**.
10. In the **User Name** box type a name.
11. In the **Organization** box type your company name.
12. Select one of the following options:
    - **Anyone who uses this computer (all users)**
    - **Only for me (User Name)**

13. Click **Next**.
14. Accept the default **Destination Folder**.

    OR

    Click **Browse** to select a different location.
15. Click **Next**.
16. Click **Install**.
17. Click **Finish**.

Procedure job aid

You can find more information about the Orchestration Designer in *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (NN44400-510).

Adding a Contact Center script or flow application

About this task

Add a Contact Center script or flow application to provide treatments for customer calls. Script applications use commands to define call treatments. Flow applications use graphical flow chart symbols to define call treatments.

Calls to the Contact Center are routed to a Master application for processing, treatments and queuing to an appropriate skillset. Avaya Aura® Contact Center answers the customer call and executes the Master application, and optional primary and secondary applications.

Applications contain instructions that determine the sequence of steps that a contact follows after the contact arrives at Contact Center. These steps can include call treatments (such as music or ringback), call routing (such as skill-based routing), or interaction with the caller (entering account numbers). Applications perform two major functions: they define the path a contact follows, and they provide treatments to a contact as the contact moves through Contact Center. You can also use the applications to track and record information about each step in the progress of a contact, and use this information to analyze how your contact center functions to improve service.

A primary application is an application executed or referenced by the Master application. Contact Center Manager Server records Master application and primary application actions in statistical records. Statistics are not recorded for secondary applications.

Avaya recommends that you modify your application to check each call for useful data. If the call has useful data or intrinsics such as CLID (Calling Line Identification), use this data to queue the call to the most appropriate skillset. If the call does not have useful data, queue the call to the appropriate default skillset.

You can use Contact Center Orchestration Designer to edit the script or flow applications. Orchestration Designer is a graphical tool that you use to create applications.

Procedure

Use the Orchestration Designer application to add a script or flow application. For more information, see *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (NN44400-510).

Procedure job aid

You can use the Contact Center Orchestration Designer graphical tool to edit the Contact Center script or flow applications.

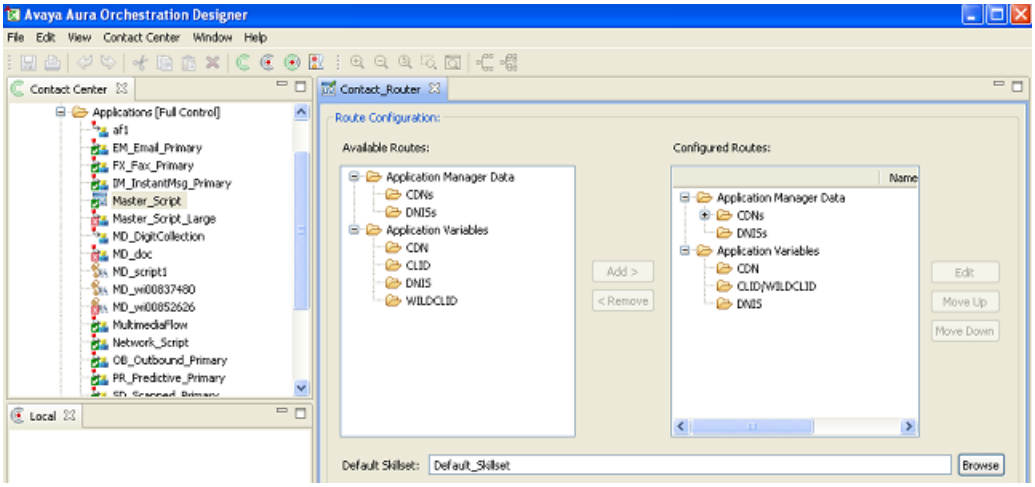


Figure 22: Example of using Orchestration Designer

Chapter 11: Certificate Authority commissioning

Certificate Authorities are used for issuing and managing certificates in software security systems that use public key technologies, such as telecoms systems that use Transport Layer Security (TLS) communication.

The Application Enablement Services (AES) server uses Transport Layer Security (TLS) communication channels for the SIP CTI connection with Avaya Aura® Contact Center. TLS is a public key encryption cryptographic protocol that helps secure a communications channel from danger or loss, and thus helps provide privacy and safety. With public key cryptography, two keys are created, one public and one private. Anything encrypted with either key can be decrypted only with the corresponding key. Thus if a message is encrypted with the server's private key, it can be decrypted only using its corresponding public key, ensuring that the data must have come from the server.

You can obtain a root certificate from a Certificate Authority. A root certificate is an unsigned public key that identifies the Root Certificate Authority (CA). Add the root certificate to the AES server and then use it to generate a Certificate Signing Request (CSR). Send the CSR and the Common Name (CN) of the AES server to your CA. The CA verifies the identity of the request and issues a signed certificate (a private key) for use by the AES server.

You must apply the root certificate and the signed client certificate from your Certificate Authority to the AES server. If using the same Certificate Authority on the Avaya Aura® Contact Center then you can apply the same root certificate to Contact Center. The Contact Center, like the AES server, must then generate a Certificate Signing Request (CSR) and get it signed by a Certificate Authority before it can establish a secure TLS SIP link. The AES and Contact Center can then communicate securely using a TLS SIP connection.

Certificate Authority deployments vary depending on IT infrastructure and security requirements. As a worked example, this section describes how to add a standalone Certificate Authority role to a Windows Server 2008 Release 2 server. And then how to use this standalone Certificate Authority to generate signed certificates.

Prerequisites to Certificate Authority commissioning

- Install Contact Center Manager Server and Contact Center Manager Administration. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).

Certificate Authority commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to commission the Certificate Authority.

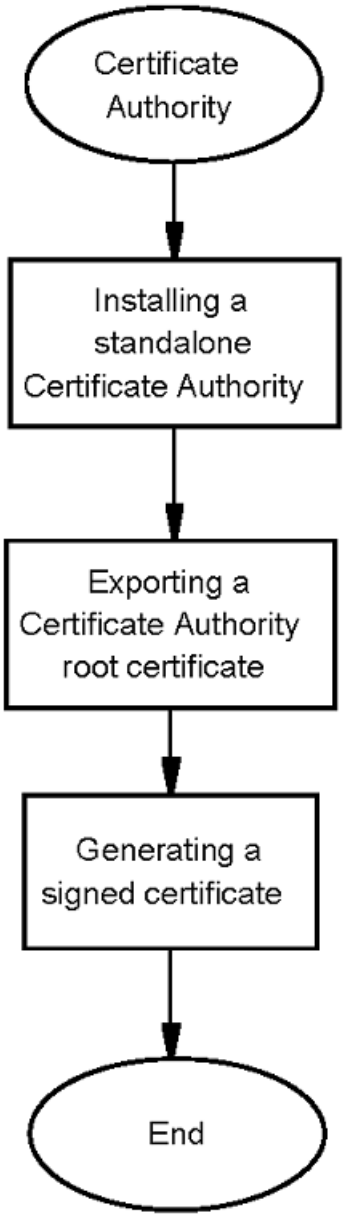


Figure 23: Certificate Authority commissioning procedures

Installing a standalone Certificate Authority

About this task

Install a standalone Certificate Authority server by adding the Certificate Authority role to a Contact Center Manager Server.

When you are installing a standalone Certificate Authority you are asked for a validity period. The default Validity Period value is 12 months (1 year). Any certificate signed by this Certificate Authority with this validity period expires after 12 months. If the certificate expires, Contact Center Manager Server loses call control of the Avaya Aura® Unified Communications platform agent phones. Certificates then have to be reassigned by the Certificate Authority before call control is reestablished.

Carefully consider the Certificate Authority Validity Period and your certificate requirements, before installing a standalone Certificate Authority.

Procedure

1. Log on to the server.
2. Click **Start** > **Administrative Tools** > **Server Manager**.
3. Under **Roles Summary**, click **Add Roles**.
4. Click **Next**.
5. Under **Roles**, select **Active Directory Certificate Services**.
6. Click **Next**.
7. On the **Active Directory Certificate Services** page, click **Next**.
8. Under **Role services**, select **Certificate Authority**.
9. Click **Next**.
10. Under **Specify Setup Type**, select **Standalone**.
11. Click **Next**.
12. Select **Root CA**.
13. Click **Next**.
14. Select **Create a new private key**.
15. Click **Next**.
16. On the **Configure Cryptography for CA** page, click **Next**.
17. On the **Configure CA Name** page, click **Next**.
18. On the **Set Validity Period** page, select a number of years appropriate to your certificate requirements.

19. Click **Next**.
20. On the **Configure Certificate Database** page, click **Next**.
21. On the **Confirm Installation Selections** page, review your selections and click **Install**.
22. After the Certificate Authority installs, click **Close**.

Procedure job aid

Example of installing a standalone Certificate Authority.

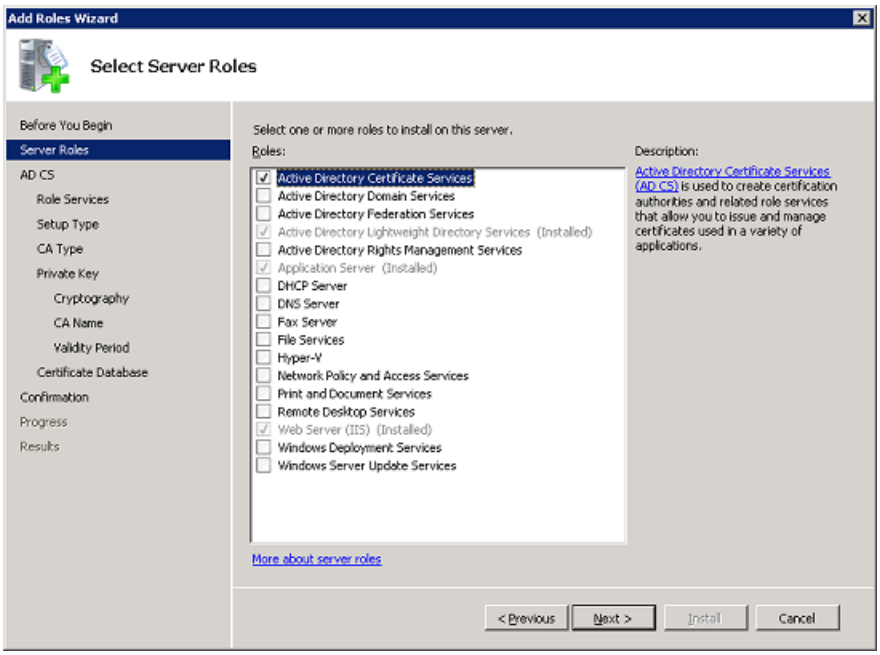


Figure 24: Example of installing a standalone Certificate Authority

Exporting a Certificate Authority root certificate

Before you begin

- Install a standalone Certificate Authority server. For more information about installing a Certificate Authority server, see Installing a standalone Certificate Authority on page 162.

About this task

Export a Certificate Authority root certificate for use in a secure system. The Certificate Authority default export folder is “C:Windows\System32”.

Important:

The Certificate Authority default export folder is “C:Windows\System32”. Contact Center Manager Server cannot import certificates from this location. When the Certificate Authority is co-resident with Contact Center Manager Server, create your own folder for certificates, and export the Certificate Authority certificates to this folder. Contact Center Manager Server can then import the certificates from your folder.

Procedure

1. Log on to the server.
2. Click **Start** > **Administrative Tools** > **Certification Authority**.
3. From the menu tree on the left side of the Certificate Authority, right-click on the Certificate Authority and select **Properties**.
4. On the **Properties** dialog, select the **General** tab.
5. Click **View Certificates**.
6. On the **Certificate** dialog, select the **Details** tab.
7. Click **Copy to File**.
   A Certificate Export Wizard appears.
8. Click **Next**.
9. Under **Select the format you want to use**, select **Base-64 encoded X.509 (.CER)**.
10. Click **Next**.
11. On the **File to Export** dialog, in the **File name** box, type the name of the Certificate Authority root certificate to export.
12. Click **Browse**, and select the export folder location.
13. Click **Next**.
14. Click **Finish**.
    A Certificate Export Wizard - The Export was successful message box appears.

15. To close the message box click **OK**.
16. Click **OK**.

Procedure job aid

Example of exporting a Certificate Authority root certificate for use in a secure system.

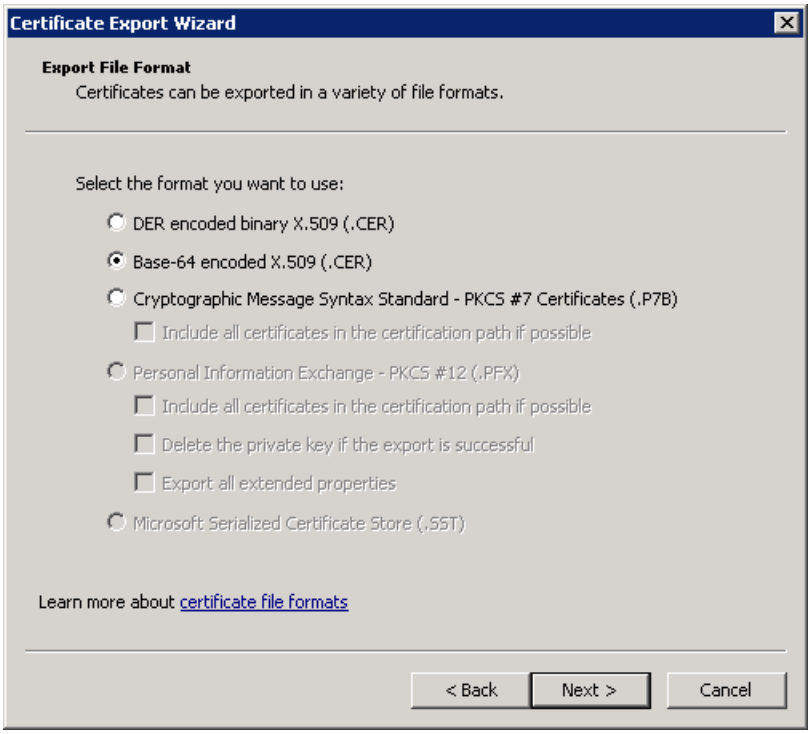


Figure 25: Exporting a Certificate Authority root certificate from a standalone Certificate Authority

Generating a signed certificate

Before you begin

- Install a standalone Certificate Authority server. For more information about installing a Certificate Authority server, see Installing a standalone Certificate Authority on page 162.
- Copy the Certificate Signing Request (CSR) text file to the standalone Certificate Authority server.

About this task

Generate a signed certificate using a Certificate Signing Request (CSR) and a standalone Certificate Authority server and then export the signed certificate for use in a secure system.

Important:

The Certificate Authority default export folder is “C:Windows\System32”. Contact Center Manager Server cannot import certificates from this location. When the Certificate Authority is co-resident with Contact Center Manager Server, create your own folder for certificates, and export the Certificate Authority certificates to this folder. Contact Center Manager Server can then import the certificates from your folder.

Procedure

1. Log on to the server.
2. Click **Start** > **Administrative Tools** > **Certification Authority**.
3. Right-click on the Certificate Authority snap-in, and select **All Tasks** > **Submit new request**.
4. On the **Open Request File** dialog, select the Certificate Signing Request (CSR) notepad text file.
5. Click **Open**.
6. From the menu tree on the left side of the Certificate Authority, select **Pending Requests**.
7. From the list of **Pending Requests**, select your request, right-click and select **All Tasks**, **Issue**.
8. From the menu tree on the left hand side of the Certificate Authority, select **Issued Requests**.
9. From the list of issued requests, select your request.
10. Right-click on the request and select **Open**.
    A Certificate Information dialog appears.
11. Select the **Details** tab.
12. Click **Copy to File**.
    A Certificate Export Wizard appears.
13. Click **Next**.
14. Under **Select the format you want to use**, select **Base-64 encoded X.509 (.CER)**.
15. Click **Next**.
16. On the **File to Export** dialog, in the **File name** box, type the name of the signed certificate to export.
17. Click **Browse**, and select the export folder location.

18. Click **Next**.
19. Click **Finish**.
    A Certificate Export Wizard - The Export was successful message box appears.
20. To close the message box click **OK**.
21. Click **OK**.

Procedure job aid

Example of generating a signed certificate.



Figure 26: Example of generating a signed certificate using a standalone Certificate Authority

Chapter 12: Contact Center Manager Server certificate commissioning

Avaya Aura® Contact Center uses industry-standard SIP and CSTA (TR/87 over SIP) interfaces to communicate with other telecoms and data systems, such as Application Enablement Services.

The SIP CTI link between Avaya Aura® Contact Center and Application Enablement Services (AES) uses the Transport Layer Security (TLS) protocol to provide secure communication. TLS uses signed security certificates to secure the link between the CCMS and the AES.

The CCMS Certificate Manager can request and store these signed security certificates. The CCMS Certificate Manager generates a Certificate Signing Request (CSR) file. A Certificate Authority uses this Certificate Signing Request file to create a signed certificate. The CCMS Certificate Manager then imports and stores Certificate Authority supplied root certificates and signed certificates.

A signed certificate must be signed by a Certificate Authority, CCMS Certificate Manager does not sign certificates.

Avaya Aura® Contact Center Release 6.2 supplies a set of default certificates for use with AES. When you install Contact Center Manager Server it creates a certificate store containing the default certificates required to communicate with AES. If you do not have access to or require a third-party Certificate Authority, you can install these Contact Center default certificates on your Application Enablement Services server to quickly setup a link between the two systems. The Avaya Aura® Contact Center default certificate Common Name (Certificate CN) is AACCSGM60.

Important:

The Contact Center default certificates for AES may not meet your organization's security requirements. Avaya recommends the you use a third party Certificate Authority or follow your organization's security policies and procedures to better secure the TLS link between Avaya Aura® Contact Center and the Application Enablement Services server.

If you plan to use the CCMS default certificates for AES, then no further CCMS certificate configuration is required, the default certificates are in the store and are ready for use.

For improved security, Avaya recommends that you obtain a root certificate from a third-party Certificate Authority or from your organization's Certificate Authority. If you plan to use a Certificate Authority and generate signed certificates you must first delete the default Contact Center Manager Server certificates and store.

This section describes how to configure Contact Center Manager Server TLS certificates to communicate securely with Application Enablement Services using a secure TLS SIP connection.

Important:

In a SIP-enabled contact center using Application Enablement Services and High Availability resiliency, the active and standby CCMS servers must both have TLS certificates in place to communicate securely with the AES server and to support High Availability switchover.

Important:

The Certificate Authority default export folder is “C:Windows\System32”. Contact Center Manager Server cannot import certificates from this location. When the Certificate Authority is co-resident with Contact Center Manager Server, create your own folder for certificates, and export the Certificate Authority certificates to this folder. Contact Center Manager Server can then import the certificates from your folder.

For more information about configuring the Application Enablement Services end of this secure TLS — SIP CTI link, see *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* (NN44400-521).

Prerequisites

- Install Contact Center Manager Server. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Commission Contact Center Manager Server. See Contact Center Manager Server commissioning procedures on page 33.

Contact Center Manager Server certificate commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to commission Contact Center Manager Server certificates.

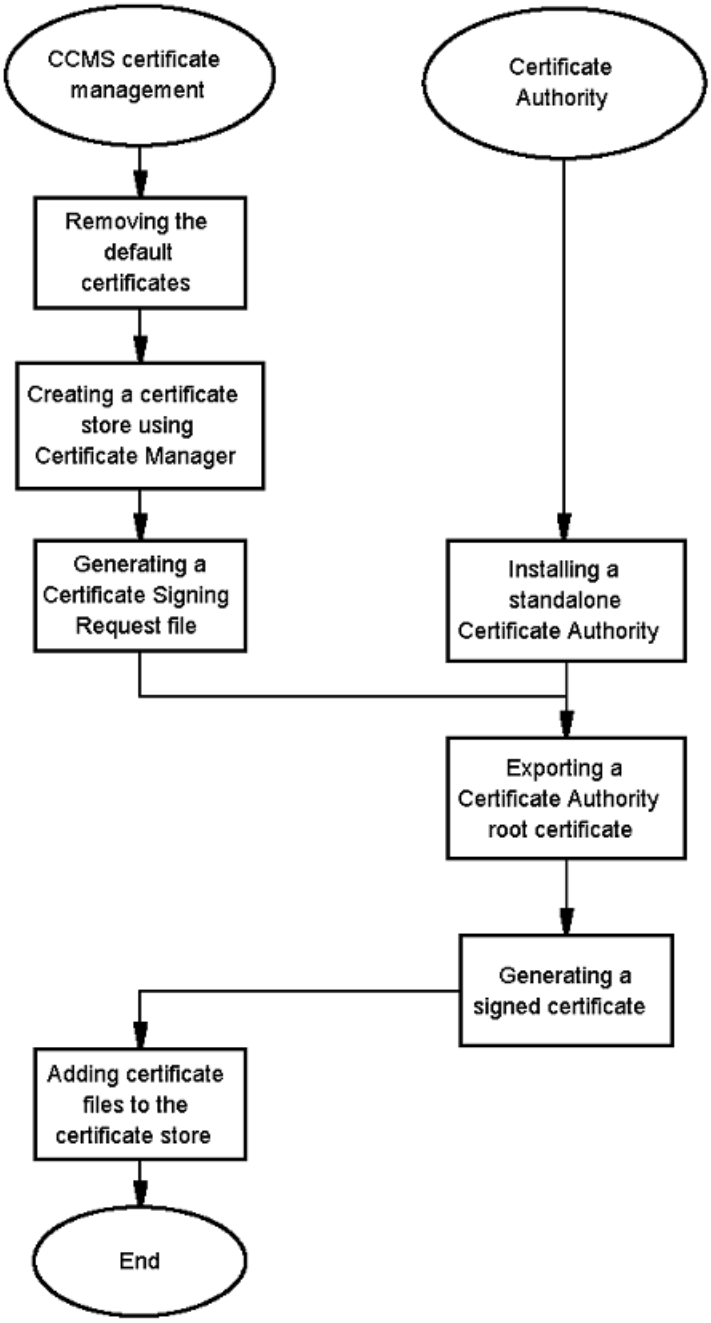


Figure 27: Contact Center Manager Server certificate commissioning procedures

Removing the default certificates

About this task

Avaya Aura® Contact Center Release 6.2 supplies a set of default certificates for use with AES. When you install Contact Center Manager Server it creates a certificate store containing the default certificates required to communicate with AES.

If you plan to use a Certificate Authority and generate signed certificates you must first delete the default Contact Center Manager Server certificates and store.

Important:

The Contact Center default certificates for AES may not meet your organization's security requirements. Avaya recommends the you use a third party Certificate Authority or follow your organization's security policies and procedures to better secure the TLS link between Avaya Aura® Contact Center and the Application Enablement Services server.

Procedure

1. Use the System Control and Monitor Utility to stop all Avaya Aura® Contact Center services.
2. Using Windows Explorer, navigate to the following default location: D:\Avaya \Contact Center\Manager Server\iccm\sgm\TLSCertificates.
3. Delete or move the **sgmKeyStore** file.
4. Delete or move the **storeInformation.txt** file.
5. Use the System Control and Monitor Utility to start Avaya Aura® Contact Center services.

Creating a certificate store using Certificate Manager

About this task

The Certificate Manager uses a store to hold Certificate Authority root certificates and signed certificates. Create the certificate store if you plan to use a Certificate Authority and generate signed certificates. The certificate store is password protected.

Procedure

1. Log on to the server where you want to create the certificate store.

2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities**.
3. Select **Certificate Manager**.
4. In the **Certificate Manager** window, from the **Create Certificates for** list, select **SIP**.
5. In the **Certificate Store** tab, in the **Full Computer Name (FQDN)** box, type the full FQDN of the server that the certificate store is on.

   Important:

   The FQDN must be the full machine name of the server that the Certificate Store resides on. The FQDN name is case-sensitive.
6. In the **Name of Organizational unit** box, type the name of the department or division within the company.
7. In the **Name of Organization** box, type the company name.
8. In the **City or Locality** box, type the name of the city or district in which the contact center is located.
9. In the **State or Province** box, type the state or province in which the contact center is located.
10. In the **Two Letter Country Code** box, type the country code in which the contact center is located.
11. In the **Certificate Store password** box, type a password to access the certificate store.
12. In the **Confirm Store password** box, type a password to access the certificate store.
13. To change the password, type the password, and click **Change Password**.
14. Select **Create Store**, the private key is created. This private key is used in the private-public key encryption.
    Certificate Manager automatically displays the Certificate Request tab, showing the newly created Certificate Signing Request file contents.
15. Select **Close**.

    Important:

    When the store has been created, the next time you start the Certificate Manager it prompts you for a password. You must enter the correct password to access Certificate Manager features and the certificate store. If you enter an incorrect password, the Certificate Manager starts, but a “No password detected” message appears if you try to access the certificate store.

Variable definitions

Name	Description
Full Computer Name (FQDN)	The host name and parent domain which fully qualifies the computer where the certificate store is to be created. The FQDN name is case sensitive. The Certificate Manager auto-populates the FQDN field by reading the name from the operating system. You can modify this field if required. Example FQDN format: computerX.DomainY.com
Name of Organizational unit	The department or division within a company.
Name of Organization	The company name.
City or Locality	The city or district in which the system is located.
State or Province	The state or province in which the system is located.
Two Letter Country Code	The country code in which the system is located.
Certificate Store password	Choose a password to access the certificate store. The password fields have been pre-populated with a default password “__avaya” (double underscore followed by name). Avaya recommends that you change this password.

Procedure job aid

The Certificate Manager creates a password protected store to hold Certificate Authority root certificates and signed certificates.

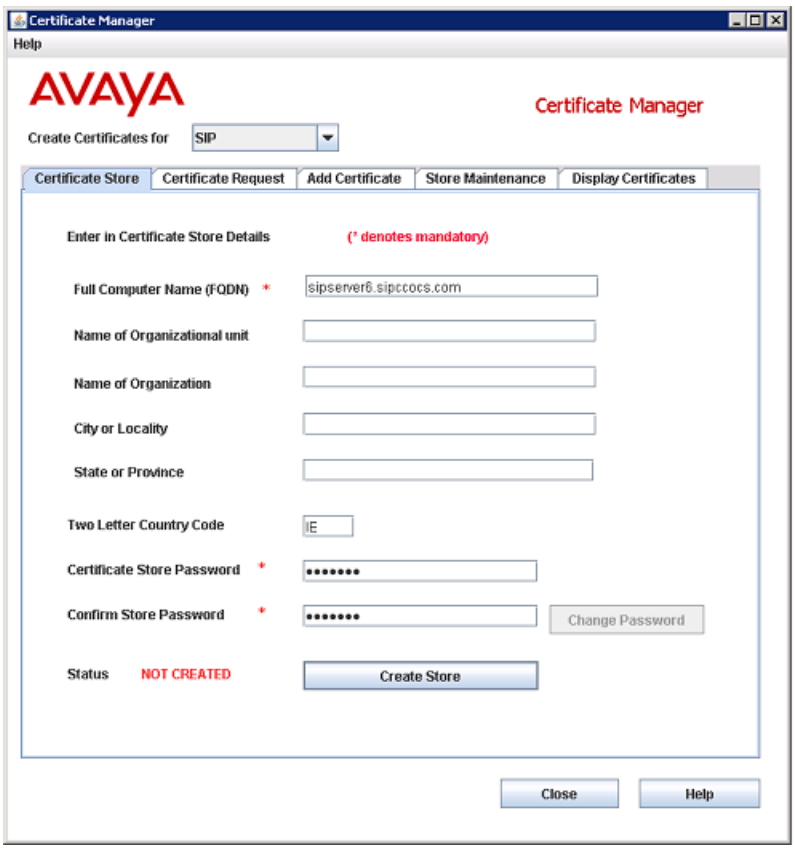


Figure 28: Example of creating a certificate store

Generating a Certificate Signing Request file

Before you begin

- Speak with your System Administrator to identify a Certificate Authority.

About this task

The Certificate Manager automatically generates a Certificate Signing Request (CSR) when it creates the certificate store. The Certificate Manager—Certificate Request tab displays the name, location, and contents of the Certificate Signing Request (CSR) file on the server. A Certificate Authority uses this Certificate Signing Request (CSR) file to generate a signed security certificate. Contact Center Manager Server uses the signed security certificate to establish a secure communication link between it and the Application Enablement Services (AES) server.

If the Certificate Signing Request (CSR) is not signed straight away, the next time you log on to the Certificate Manager the CSR file is still present and the Signing Request Status field shows the CSR status as Pending. When the CSR is signed and placed into the certificate

store via the “Add Certificate Tab” the status changes to “Signed” to indicate that this CSR has been signed.

Procedure

1. Log on to server containing the store.
2. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities**.
3. Select **Certificate Manager**.
4. Select **Certificate Request** tab.
5. Check the status of the Certificate Signing Request (CSR). If **Signing Request Status** is set to **Pending**, have the CSR signed by a Certificate Authority.
6. Select **Close**.

   Important:

   After you perform this procedure, the certificate must be signed by a Certificate Authority. Contact your System Administrator for the preferred method of processing the signed certificate request file to obtain a signed certificate. When you receive the signed certificate, save it on the server containing the Certificate Manager.
7. Retrieve the Certificate Signing Request file from the **File location** shown on the **Certificate Request** tab.

Variable definitions

Name	Description
Certificate Store Status	Indicates if the Certificate Store is created.
Signing Request Status	Indicates if the generated Certificate Signing Request that appears is signed and added back into the store. Pending: Certificate Manager is waiting for a signed certificate to be added back into the store. Signed: Certificate Manager added the certificate signed by a specific Certificate Authority into the store.
File Location	Location of the Certificate Signing Request file.

Name	Description
Contents	Displays the contents of the Certificate Signing Request file. You can copy this directly from the field and have it signed.

Procedure job aid

The Certificate Manager generates a Certificate Signing Request. A Certificate Authority uses this Certificate Signing Request (CSR) file to generate a signed certificate.

For more information about using a Certificate Signing Request (CSR) file to generate a signed certificate, see Generating a signed certificate on page 165.

For more information about generating the Certificate Authority root certificate required by Contact Center Manager Server, see Exporting a Certificate Authority root certificate on page 164.



Figure 29: Example of creating a Certificate Signing Request for Contact Center Manager Server

Adding certificate files to the certificate store

Before you begin

- Obtain a Certificate Authority root certificate. For more information about obtaining a CA root certificate, see Exporting a Certificate Authority root certificate on page 164.
- Obtain a signed certificate from the same Certificate Authority that generated the Certificate Authority root certificate. For more information about obtaining a signed certificate, see Generating a signed certificate on page 165.
- Save the certificate files on the Contact Center Manager Server server.

About this task

The Certificate Manager can add both Certificate Authority root certificates and signed certificates to the Contact Center Manager Server certificate store. Contact Center Manager Server requires a signed certificate and a corresponding Certificate Authority root certificate to communicate securely with Application Enablement Services (AES).

For more information about generating a Certificate Authority root certificate, see Exporting a Certificate Authority root certificate on page 164.

For more information about generating a signed certificate, see Generating a signed certificate on page 165.

There are two options when adding CA root and signed certificates.

Automatically adding certificates :

You can select a folder that contains signed and root certificates. Certificate Manager accesses this folder and automatically determines which are signed certificates and which are root certificate and then adds them to the certificate store accordingly.

Important:

Certificate Manager attempts to import all files and certificates it finds in the certificate folder. Ensure that the certificate folder contains only Certificate Authority root certificates and signed certificates.

Manually adding certificates :

For manually added certificates, you can browse for individual signed and root CA certificates and add them to the certificate store, one at a time. Certificate Manager checks the certificates and does not add signed certificates as root CA certificates.

Procedure

1. Log on to server containing the certificate store.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities**.
3. Select **Certificate Manager**.

4. In **Store Access**, type the certificate store password.
5. Click **OK**.
6. In the **Certificate Manager** window, in the **Create Certificates for** list, select **SIP**.
7. Select **Add Certificate** tab.
8. Select the method to add certificates.

   Select **Add Certificates Automatically**, and skip to step 9.

   OR

   Select **Add Certificates Manually**, and skip to step 13.
9. Click **Browse**, and navigate to the directory that contains the certificates.
10. Select the directory.
11. Click **Add all Certificates**.
12. Skip to step 16.
13. In the **Add Root Certificate** or **Add Signed Certificate** section as appropriate, click **Browse**, and navigate to the required certificate.
14. To manually add a Certificate Authority root certificate, click **Add CA Certificate**.
15. To manually add a signed certificate, click **Add Signed Certificate**.
16. Select **Close**.

Variable definitions

Name	Description
Certificate Store password	Password to access the certificate store.
Add Certificates Automatically	Certificate Manager automatically determines which certificates are signed and which are root certificate and then adds them to the certificate store accordingly.
Select folder	The folder from which Certificate Manager automatically loads certificates.
Add Certificates Manually	Manually add certificates, one at a time.
Add Root Certificate	The name and location of the root certificate. Root Certificate Authority certificates must be in Base64 format.

Name	Description
Add Signed Certificate	The name and location of the signed certificate. Signed certificates must be in DER format.

Procedure job aid

The same root certificate must be applied to the Application Enablement Services so that CCMS can communicate securely with it using TLS. For more information about configuring Application Enablement Services certificates, see *Avaya Aura® Contact Center Configuration – Avaya Aura® Unified Communications Platform Integration* (NN44400-521).

Removing a certificate file from the certificate store

Before you begin

- Save the certificate files on your certificate store computer.

About this task

You can remove the certificates added to the store manager by using the Store Maintenance tab of the Certificate Manager.

Procedure

1. Log on to server containing the store.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities**.
3. Select **Certificate Manager**.
4. In **Store Access**, type the certificate store password.
5. Click **OK**.
6. In the **Certificate Manager** window, in the **Create Certificates for** list, select **SIP**.
7. Select the **Store Maintenance** tab.
8. In **Certificates**, Certificate Manager lists all certificates in the store.
9. Select the certificate to remove.
10. Select **Remove**, to remove the selected certificate from the store.
11. Select **Close**.

Variable definitions

Name	Description
Certificate Store password	Password to access the certificate store.
Certificates	List of certificates saved in the store.

Procedure job aid

Use the Certificate Manager – Store Maintenance tab to view all certificates in the certificate store, and to remove one or more selected certificates.

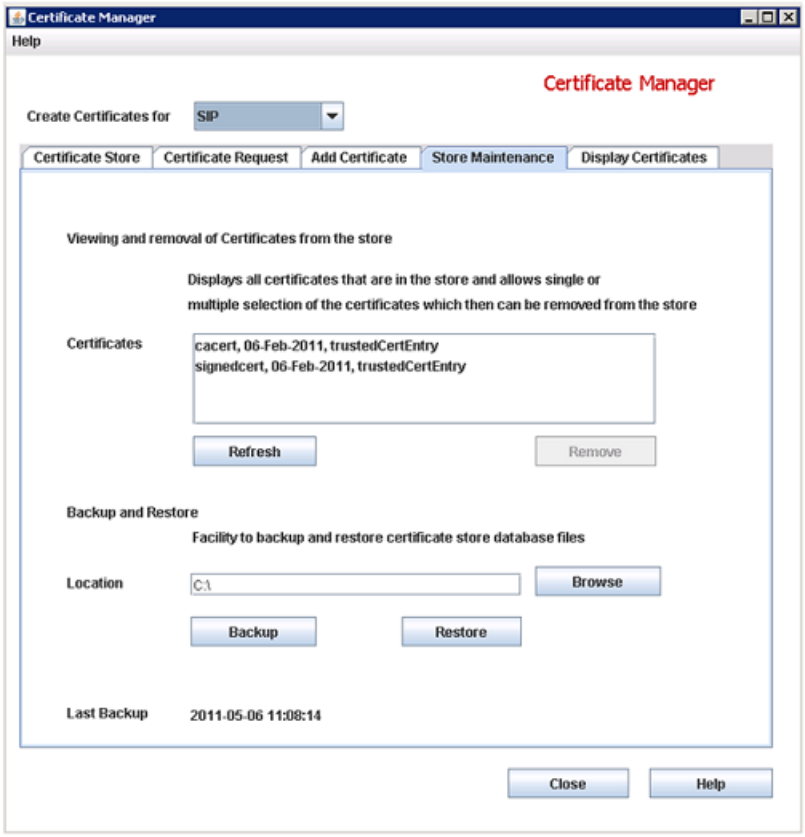


Figure 30: Example of removing a certificate from the certificate store

Examining a certificate file in the certificate store

Before you begin

- The certificate store must contain one or more certificate.

About this task

View the certificates in the store using the Certificate Manager Display Certificates tab.

Procedure

1. Log on to server containing the store.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities**.
3. Select **Certificate Manager**.
4. In **Store Access**, enter the certificate store password.
5. Click **OK**.
6. In the **Certificate Manager** window, in the **Create Certificates for** list, select **SIP**.
7. Select the **Display Certificates** tab.
8. Select **List**, to list all stored certificates in the store.
9. Select a certificate.
   The details of the certificate are displayed.
10. Select **Close**.

Variable definitions

Name	Description
Certificate Store password	Password to access the certificate store.
Select Certificate	List of certificates saved in the store.
Certificate Detail	Display details of the certificate.

Procedure job aid

Use the Certificate Manager – Display Certificates tab to view certificate details.

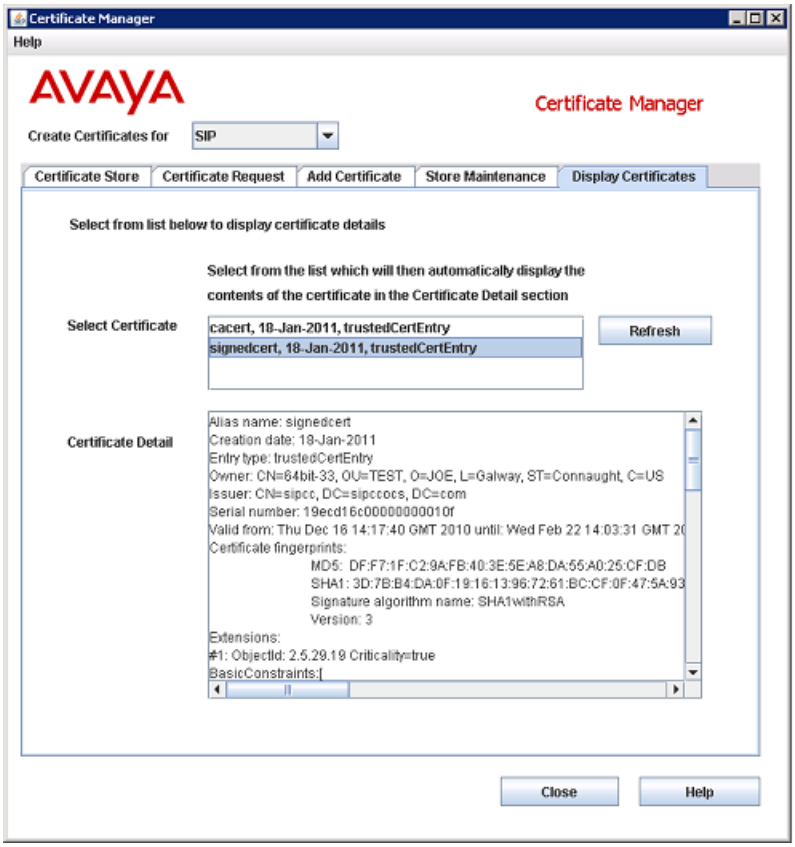


Figure 31: Example of examining a certificate file in the certificate store

Chapter 13: Security Framework commissioning

Perform the procedures in this chapter to commission the Security Framework after you install Security Framework server software.

Use the Unified Communication Management utility to configure the Security Framework server software after you install it.

Prerequisites for Security Framework commissioning

- Install or upgrade the Contact Center Manager Administration software. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Install the Security Framework either co-resident with Contact Center Manager Administration or on a stand-alone server.
- Read *Avaya Aura® Contact Center Fundamentals* (NN44400-110).
- Ensure that you have administrator privileges on the server on which you installed the Contact Center Manager Administration server software.
- Ensure that you have administrator privileges on the server on which you installed the Security Framework software.

Security Framework commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to commission Security Framework.

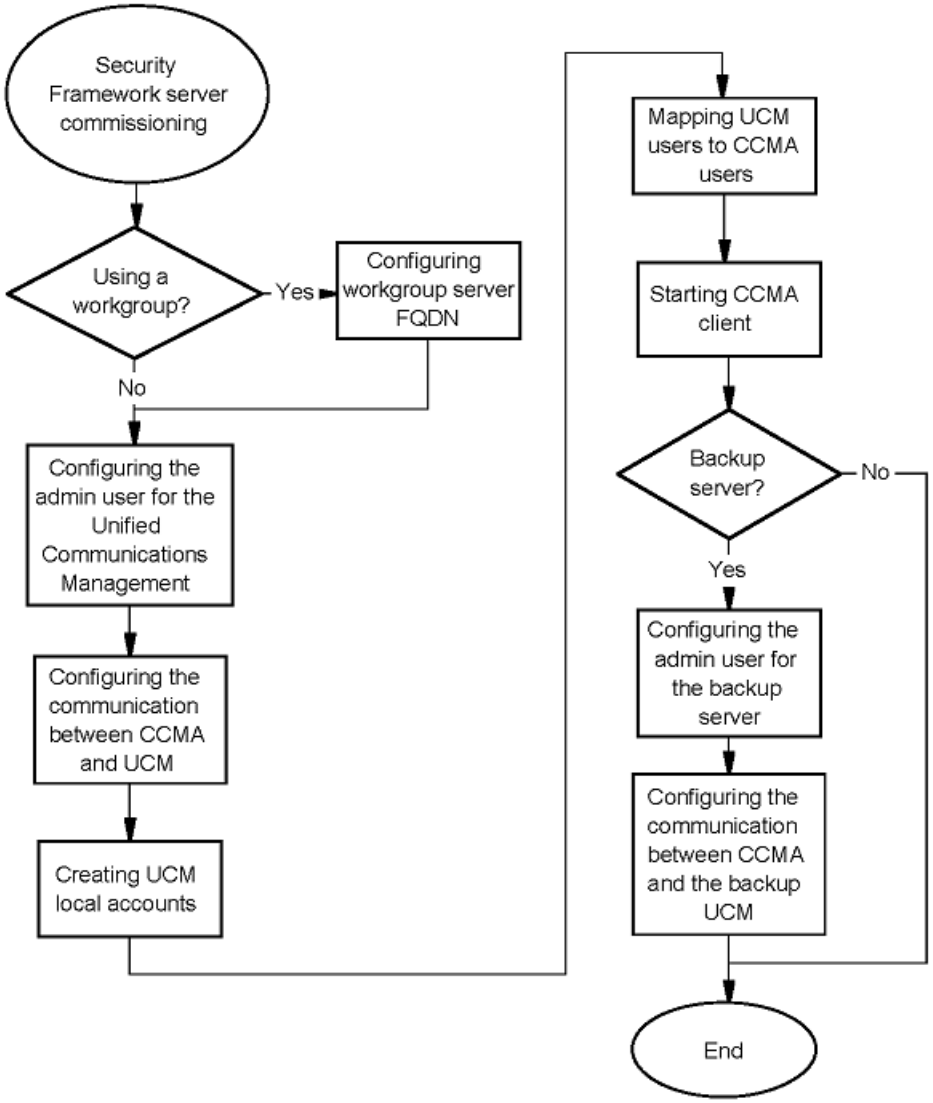


Figure 32: Security Framework commissioning procedures

Job aid: Timing

The estimated time to commission Security Framework is 1 hour.

Configuring workgroup server Fully Qualified Domain Name

About this task

Security Framework supports domains and workgroups. When using a workgroup, you must configure the Fully Qualified Domain Name (FQDN) of the Contact Center Manager Administration server and the Security Framework server so they can communicate with each other.

Important:

Skip this procedure if the Security Framework server is in a domain.

The Primary DNS suffix of a server specifies the DNS suffix to be appended to the name of a server when completing its fully qualified domain name (FQDN). The Contact Center Manager Administration server and the Security Framework server must both have the same Primary DNS suffix name.

Important:

You must restart the server after changing the Primary DNS suffix.

Procedure

1. Log on to the Security Framework workgroup server.
2. Select **Start** > **Computer** > **System properties**.
3. On the **System** dialog box, click **Change settings**.
4. On the **System Properties** dialog box, click **Change**, **More**.
5. In the **Primary DNS suffix of this computer** box, type the Fully Qualified Domain Name (FQDN) for the workgroup.

   For example type `myWorkgroup.com`.
6. Click **OK**.
7. On the **Computer Name/Domain Changes** dialog box, confirm that the **Full computer name** now displays the Fully Qualified Domain Name (FQDN) for the workgroup server. For example, `myServerName.myWorkgroup.com`.
8. Click **OK**.
9. On the server restart notice dialog, click **OK**
10. Click **Close**.
11. Click **Restart Now**.

12. Repeat this procedure on the Contact Center Manager Administration server.

Configuring the admin user for the Unified Communication Manager

About this task

Log on to the Security Framework Unified Communication Manager (UCM) for the first time and configure the administrator account used to secure Web traffic before you set up users.

Procedure

1. Log on to the server where the Security Framework is installed.
2. Start Internet Explorer.
3. In the URL box, type `https://FQDN:<security port>`.

   The FQDN is the fully qualified domain name for your server.
4. If the Digital Certificate window appears, click **OK**.
5. If any **Security Alert** message boxes appear, click **Yes**.
6. In the **User ID** box, type a local user name you use to log on to the server.
7. In the **Password** box, type the password for the account you use to log on to the server.
8. Click **Log In**.
9. Click **Security Configuration**.
10. Verify the Fully Qualified Domain Name and the Web Server IP address by selecting **Yes**.
11. Click **Next**.
12. Select the **Primary security server**.
13. Click **Next**.
14. In the **Administrator password** box type a password for the admin account for the Unified Communication Management utility.
15. In the **Confirm Administrator password** box, retype the password.
16. Click **Next**.
17. In the Certificate Information window, in the **Friendly name** box, type a name for the certificate.
18. From the **Bit length** list, select the bit length.

19. In the **Organization** box, type the name for the organization using the security certificate.
20. In the **Organizational unit** box, type the name of the group of users using the security certificate.
21. In the **Common name** box, type the fully qualified domain name for the server.
22. From the **Country/Region** list, select your country or region.
23. In the **State/Province** box, type the name of your state or province.
24. In the **City/Locality** box, type the name of your city.
25. Click **Finish**.
26. After the configuration completes, click **Restart**.

Variable definitions

Name	Description
Admin user password	The administrator password using standard password definitions for your system. When a user logs on with the admin password, they are forced to change the default password.
Bit length	Number of bits to use to encrypt the security certificate. You can choose from the predefined values of 512, 1024, and 2048. The more bits required for encryption, the more CPU cycles are required to process the access.
City/Locality	The city or locality in which you are located.
Common name	The fully qualified domain name (FQDN) of the server. For Windows, it is a combination of the COMPUTERNAME and USERDNSDOMAIN environment variables. This must match the host name of the system for the certificate.
Country/Region	The country or region in which you are located.
Friendly name	Identify the security certificate using a name.
Organization	Your company name.

Name	Description
Organizational unit	Unit within the company for the security certificate.
State/Province	The state or province in which you are located.
<security port>	The security port number for the Security Framework/Unified Communication Manager. The default value is 8443.

Configuring the communication between CCMA and UCM

Before you begin

- Commission the CCMA server. See Contact Center Manager Administration commissioning on page 121.
- Configure the password for the admin user of the Unified Communication Manager. See Configuring the admin user for the Unified Communication Manager on page 188.
- Ensure that the Security Framework server is also added as a trusted site in Internet Explorer on the Contact Center Manager Administration server.

About this task

Configure the communication information between Contact Center Manager Administration (CCMA) and the Unified Communication Manager (UCM) to ensure that the two applications work with each other.

Procedure

1. Log on to the server on which you installed the Contact Center Manager Administration server software.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Configuration**.
3. In the Configuration window, in the left pane, expand **Avaya** and **Applications**.
4. Select **Security Settings**.
5. In the right pane, click **Security Settings**.
6. In the **Security Details** dialog box, choose the location of your Primary Security Server.
7. In the **Web Site Identifier** list, select **Default Web Site, 1**.
8. For **CCMA Server Protocol**, if SSL is enabled, you can select **https**; otherwise, **http** is selected by default.

9. Accept the default **IIS Port Number**.
10. If the Security Framework Server is installed on another server, type the CCMA FQDN in the **Security Server FQDN** box, in the **Security Server Details** section.
11. In the **Security Server Port Number** box, type the security server port number.
12. In the **Cache Interval** box, type a number. This represents the number of local sessions of information cached on the server.
13. Click **Enable**.
14. On the **Information** box, click **Yes**.
15. Click **OK** to accept the updates.
16. Click **Close**.

Variable definitions

Name	Description
Security Details	Information about whether the Security Framework is installed on the same server as the Contact Center Manager Administration server or not. You can choose from two options: • Other server—Security Framework and CCMA are on separate servers. • On this server—Security Framework and CCMA are installed on the same server.
Security Server Details	The fully qualified domain name for the Contact Center Manager Administration server.
Cache Interval	The number of local sessions of information cached on the server.
Security Server Port Number	The port number used on the Security Framework server for communication between the Security Framework and the Contact Center Manager Administration server. The default number is 8443.
CCMA Server Protocol	The protocol used to communicate between the Contact Center Manager Administration server and the internet. If SSL is enabled, select https.

Name	Description
	Otherwise, http is selected by default.

Creating Unified Communication Management local accounts

Before you begin

- Know the admin password you configured in Configuring the admin user for the Unified Communication Manager on page 188 for the Unified Communication Manager.
- Configure the server security settings. See Configuring the communication between CCMA and UCM on page 190.

About this task

Create local administrative users in Unified Communication Manager for authentication and authorization of application users in the Avaya Aura® Contact Center. Administrators have a single sign-on to the security framework to minimize the necessity for users to provide separate logon credentials across multiple applications.

The first account you must create is a local account on the Unified Communication Network that is associated the webadmin account in Contact Center Manager Administration.

Procedure

1. Log on to the server where the Security Framework is installed.
2. Start **Internet Explorer**.
3. In the URL box, type `https://FQDN:<security port>`.

   The FQDN is the fully qualified domain name for your server.
4. If the Digital Certificate window appears, click **OK**.
5. If any **Security Alert** message boxes appear, click **Yes**.
6. In the **User ID** box, type admin.
7. In the **Password** box, type the administrator password for the Unified Communication Manager.
8. Click **Log In**.
9. Under **User Services**, select **Administrative Users**.
10. Click **Add**.
11. Type the account details for your user as required.

    Your first local account is associated with the webadmin account to access Contact Center Manager Administration.

12. Beside **Authentication type**, select **Local**.
13. Click **Save and Continue**.
14. Click **Finish**.

Variable definitions

Name	Description
User ID	The user ID for the new Unified Communication Management user.
Authentication Type	Type of access granted to the user. You can choose local access or external.
Full Name	The name representing the user in the Unified Communication Management.
Temporary password	The temporary password for the new Unified Communication Management user. The password must be changed when the user logs on to the UCM for the first time.

Mapping Unified Communication Management users to CCMA users

About this task

Map all Unified Communication Manager users to Contact Center Manager Administration users to ensure the single sign on feature is enabled for all applications.

When you create users in Contact Center Manager Administration, you can use this utility to map CCMA users to UCM users.

Procedure

1. On the CCMA server, click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Configuration**.
2. In the Configuration window, in the left pane, expand **Avaya** > **Applications**.
3. Select **CCMA User Migration**.
4. In the right pane, click **CCMA User Migration**.
5. Under **Search Type**, select **Local Security Server** or **Domain**.

6. If you selected **Local Security Server**, enter the username and password of a local security server administrative user account.
7. Under **Search Options**, specify the details for the users you want to find.

   OR

   On the right side of the window, click **List All**.
8. Under the **Map User Accounts** list, select a configured Unified Communication Manager account you want to map.
9. Under the **Unassigned CCMA Users** list, select a CCMA user that you want to map to the Unified Communication Manager account.
10. Click **Map User**.
11. Click **Save**.
12. Click **Close**.

Variable definitions

Name	Description
Search Type	Search for users configured on the system. Local Security Server—find all accounts configured on the server. Domain—find all external users on a domain, such as an LDAP or database.
Local Security Server Hostname	Available only if you select Local Security Server. Type the host name of the local security server.
User ID	Available only if you select Local Security Server. Type the user name of a local security server user account that has administrative privileges.
Password	Available only if you select Local Security Server. Type the password of the local security server user.
Domain Details: Server IP (or DNS)	Available only if you select Domain. Type the IP address or domain name of a server from which to get the user names (For example, an LDAP or user database server.

Name	Description
Domain Account: User ID	Available only if you select Domain. Type a the user name of a domain user with administrative privileges.
Domain Account: Password	Available only if you select Domain. Type the password for the domain user.

Starting Contact Center Manager Administration client

Before you begin

- Map the CCMA user accounts in the Unified Communication Management utility. See Mapping Unified Communication Management users to CCMA users on page 193.
- Ensure that the Security Framework server is also added as a trusted site in Internet Explorer.

About this task

Start Contact Center Manager Administration client in a manner different from that described previously now that the Security Framework is installed.

Procedure

1. On the CCMA server, start Internet Explorer.
2. Type `https://FQDN:<security port>`.
3. Log on using an account mapped in the Unified Communication Management utility.
4. If you are prompted to change your password, change the password for the user account.

Configuring the admin user for the backup server

About this task

Configure the admin user for the optional secondary security framework server. You must configure the administrator account that is used to secure Web traffic before you set up users.

You can configure UCM users only on the primary security server. If your system security is managed by the backup Security Framework server, then you cannot change a user account.

Procedure

1. Log on to the server where the Security Framework is installed.
2. Start Internet Explorer.
3. In the URL box, type `https://FQDN:<security port>`.
   The FQDN is the fully qualified domain name for your server.
4. If the Digital Certificate window appears, click **OK**.
5. If any **Security Alert** message boxes appear, click **Yes**.
6. In the **User ID** box, type a local user name you use to log on to the server.
7. In the **Password** box, type the password for the account you use to log on to the server.
8. Click **Log In**.
9. Click **Security Configuration**.
10. Verify the Fully Qualified Domain Name and the Web Server IP address by selecting **Yes**.
11. Click **Next**.
12. Select the **Backup security server**.
13. Click **Next**.
14. In the **Address of the Primary security server** box, type the fully qualified domain name and security port of the primary security server.
15. Click **Next**.
16. Type the **Primary Security server user ID** and the **Primary Security server password**.
17. Click **Next**.
18. In the Certificate Information window, in the **Friendly name** box, type a name for the certificate.
19. From the **Bit length** list, select the bit length.
20. In the **Organization** box, type the name for the organization using the security certificate.
21. In the **Organizational unit** box, type the name of the smaller group of users using the security certificate.
22. In the **Common name** box, type the fully qualified domain name for the server.
23. From the **Country/Region** list, select your country or region.
24. In the **State/Province** box, type the name of your state or province.
25. In the **City/Locality** box, type the name of your city.

26. Click **Finish**.
27. After the configuration completes, click **Restart**.

Variable definitions

Name	Description
Admin user password	The administrator password using standard password definitions for your system. When a user logs on with the admin password, they are forced to change the default password.
Bit length	Number of bits to use to encrypt the security certificate. You can choose from the predefined values of 512, 1024, and 2048. The more bits required for encryption, the more CPU cycles are required to process the access.
City/Locality	The city or locality in which you are located.
Common name	The fully qualified domain name (FQDN) of the server. For Windows, it is a combination of the COMPUTERNAME and USERDNSDOMAIN environment variables. This field must match the host name of the system for the certificate.
Country/Region	The country or region in which you are located.
Friendly name	Identify the security certificate using a name.
Organization	Your company name.
Organizational unit	Unit within the company for the security certificate.
State/Province	The state or province in which you are located.
<security port>	The security port number for the Security Framework Unified Communication Manager. The default value is 8443.

Configuring the communication between CCMA and the backup UCM

Before you begin

- Commission the CCMA server. See Contact Center Manager Administration commissioning on page 121.
- Configure the password for the admin user of the backup Unified Communication Manager (UCM). See Configuring the admin user for the backup server on page 195.
- Ensure that the Security Framework server is also added as a trusted site in Internet Explorer on the Contact Center Manager Administration server.

About this task

Configure the communication information between Contact Center Manager Administration (CCMA) and the backup Unified Communication Manager (UCM) to ensure that the two applications work together.

Procedure

1. Log on to the server on which you installed the Contact Center Manager Administration server software.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Administration** > **Configuration**.
3. In the Configuration window, in the left pane, expand **Avaya** and **Applications**.
4. Select **Security Settings**.
5. In the right pane, click **Security Settings**.
6. In the **Resiliency Security Details** box, select **Failover Security Server**.
7. Click **Add**.
8. In the **Security Server Details** section, in the **Security Server FQDN** box, type in the CCMA FQDN.
9. In the **Port Number** box, type the port number. The default is 8443.
10. Click **Add**.
11. Click **Enable**.
12. On the **Information** box, click **Yes**.
13. Click **OK** to accept the updates.
14. Click **Close**.

Variable definitions

Name	Description
Security Details	Information about whether the Security Framework is installed on the same server as the Contact Center Manager Administration server or not. You can choose from two options: • Stand-alone security server—Security Framework and CCMA are on separate servers. • Co-res security server—Security Framework and CCMA are installed on the same server.
Security Server Details	The fully qualified domain name for the Contact Center Manager Administration server.
Cache Interval	The number of local sessions of information cached on the server.
Security Server Port Number	The port number used on the Security Framework server for communication between the Security Framework and the Contact Center Manager Administration server. The default number is 8443.
CCMA Server Protocol	The protocol used to communicate between the Contact Center Manager Administration server and the internet. If SSL is enabled, select https. Otherwise, http is selected by default.

Chapter 14: Contact Center Manager Administration client commissioning

After you install Contact Center Manager Administration server software, commission the client PCs to access Contact Center applications.

Prerequisites for client commissioning

- Install or update the Contact Center Manager Administration server software. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311) or *Avaya Aura® Contact Center Upgrade and Patches* (NN44400-410).
- Install or update the required client applications. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311) or *Avaya Aura® Contact Center Upgrade and Patches* (NN44400-410).
- Install Microsoft Internet Explorer 7.0 or later (32-bit version only). Contact Center Manager Administration supports only the 32-bit version of Microsoft Internet Explorer.

Client commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to commission the client.

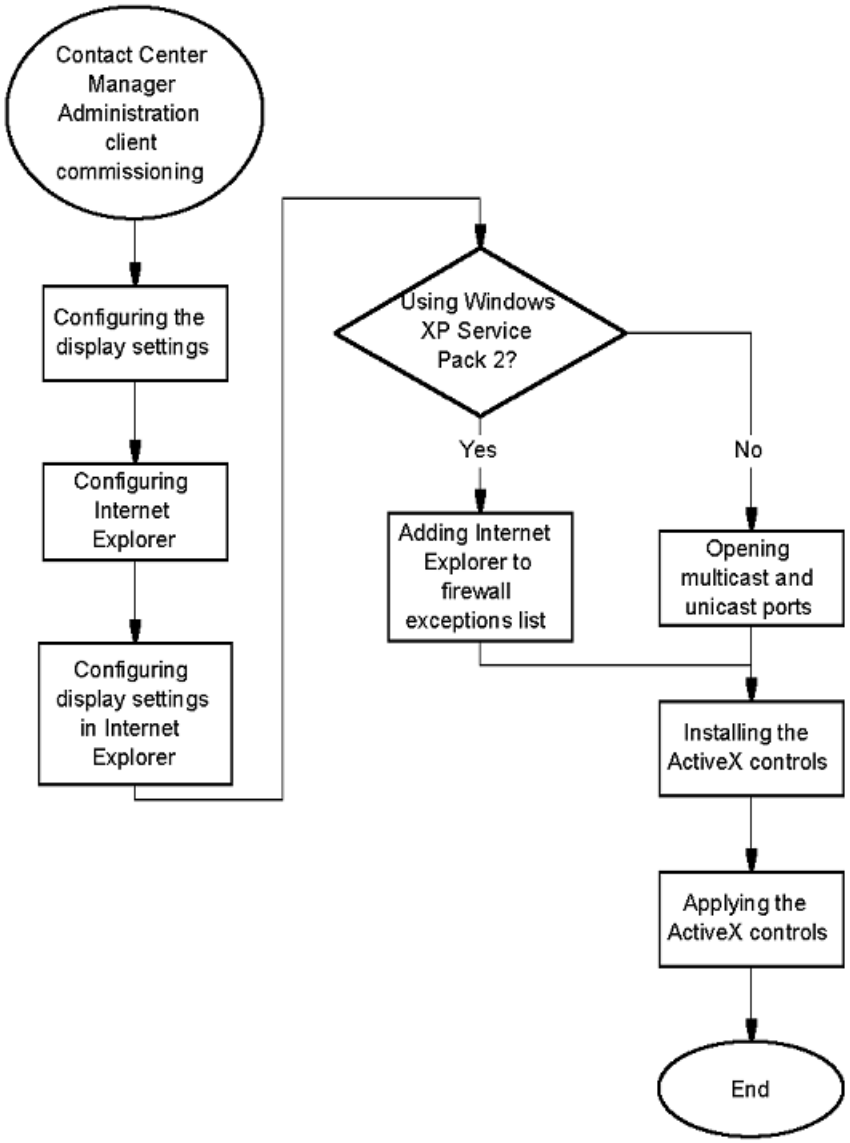


Figure 33: Client commissioning procedures

Job aid: Timing

The estimated time to commission the client is 20 minutes.

The time can vary depending on the server, network infrastructure, and your confidence level with the software.

Configuring the display settings

About this task

Configure the display settings on each client PC so that all Contact Center Manager Administration components such as reports appear correctly in the browser window.

Procedure

1. On the client PC, click **Start** > **Control Panel** > **Display**.
2. In the **Display Properties** dialog box, click the **Appearance** tab.
3. From the **Font size** list, select **Normal**.

   Important:

   If you do not select Normal, some items may not display correctly in the browser.
4. Click the **Settings** tab.
5. Configure the screen resolution to **1024 X 768**.

   Important:

   Avaya recommends this resolution to accommodate Real-Time Display billboard collections.
6. Click **Apply**.
7. Click **OK**.

Configuring Internet Explorer

About this task

Configure Internet Explorer on each client to access Contact Center Manager Administration.

Install Microsoft Internet Explorer 7.0 or later (32 bit version only). Contact Center Manager Administration supports only the 32 bit version of Microsoft Internet Explorer.

If you are using Security Framework on your client, ensure that the Security Framework server is also added as a trusted site in Internet Explorer.

Procedure

1. Start Internet Explorer.
2. From the menu, select **Tools** > **Internet Options**.
3. In the **Internet Options** dialog box, click the **Security** tab.
4. Click the **Trusted Sites** icon.
5. Click **Custom Level**.
6. In the **Security Settings** dialog box for trusted sites, under the **.NET Framework-reliant components** heading, select **Enable** for the following:
   - **Run components not signed with Authenticode**
   - **Run components signed with Authenticode**
7. Under the **ActiveX controls and plug-ins** heading, select **Enable** for the following:
   - **Automatic prompting for ActiveX controls**
   - **Run ActiveX Controls and plug-ins**
   - **Script ActiveX Controls marked safe for scripting**
8. Under the **Downloads** heading, select **Enable** for the following:
   - **Automatic prompting for file downloads**
   - **File download**
9. Under the **Miscellaneous** heading, for **Allow script-initiated windows without size or position constraints**, select **Enable**.
10. Under the **Miscellaneous** heading, for **Allow websites to open windows without address or status bars**, select **Enable**. (Applies to Internet Explorer 7.0 and later.)
11. Click **OK**.
12. If you enabled ActiveX options, when a message appears asking you to confirm your choice, click **Yes**.
13. Click the **Trusted Sites** icon.
14. Click **Sites**.
15. In the **Trusted sites** dialog box, clear the **Require server verification {https:} for all sites in this zone** check box.
16. In the **Add this Web site to the zone** box, type the server name (not the IP address) for your Contact Center Manager Administration server.

    OR

    If you used the fully qualified domain name when you installed Contact Center Manager Administration on the Contact Center Manager Administration server, in the **Add this Web site to the zone** box, type the fully qualified domain name.
17. Click **Add**.

18. In the **Add this Web site to the zone** box, type the server name (not the IP address) for your Contact Center Multimedia server.
19. Click **Add**.
20. If your contact center includes a Predictive Reporting server, in the **Add this Web site to the zone** box, type the server name (not the IP address) for your Predictive Reporting server.
21. Click **Add**.
22. Click **Close** to return to the **Internet Options** dialog box.
23. Click the **Privacy** tab.
24. In the **Pop-up Blocker** section, select the **Block pop-ups** check box.
25. Click **Settings**.
26. In the **Pop-up Blocker Settings** dialog box, in the **Address of website to allow** box, type the Contact Center Manager Administration URL, http://<server name>/.
27. Click **Add**.
28. Click **Close**.
29. In the **Internet Options** dialog box, click the **Advanced** tab.
30. Under **Browsing**, clear the **Reuse windows for launching shortcuts** check box.
31. If HTTPS and SSL are enabled, and if you are using Internet Explorer 9.0, under **Security** clear the **Do not save encrypted pages to disk** check box.
32. Click **Apply**.
33. Click **OK** to exit the **Internet Options** dialog box.
34. Restart Internet Explorer to activate your changes.

Configuring display settings in Internet Explorer

About this task

Configure display settings for Western European (ISO) countries in Internet Explorer to properly view characters and windows.

Procedure

1. Open Internet Explorer.
2. Click **View** > **Encoding** > **Western European (ISO)**.

3. Close Internet Explorer.

Adding Internet Explorer to the firewall exceptions list

Before you begin

- Ensure that the client PC is running Windows XP Service Pack 2 or later.
- Ensure that the Windows Firewall/Internet Connection Sharing (ICS) is running.

About this task

Add Internet Explorer to the firewall exceptions list if the client is running Windows XP Service Pack 2 to ensure data can move between the clients and the server for reporting.

Alternatively, you can open multicast and unicast ports. To open multicast and unicast ports, see Opening multicast and unicast ports on page 206.

Procedure

1. On the client PC, click **Start** > **Control Panel** > **Windows Firewall**.
2. Click the **Exceptions** tab.
3. In the **Programs and Services** list, select **Internet Explorer**.
4. If Internet Explorer is not listed, click **Add Program**.
5. In the **Add a Program** dialog box, click **Internet Explorer**.
6. Click **OK** to close the **Add a Program** dialog box.
7. Click **OK**.

Opening multicast and unicast ports

Before you begin

- Ensure that the client PC is not running Windows XP Service Pack 2 or later.

About this task

Open multicast and unicast ports to ensure data can move between the clients and the server for reporting.

If the client PC is running Windows XP Service Pack 2 or later, you can add Internet Explorer to the firewall exceptions list, or open a specific set of ports. See Adding Internet Explorer to the firewall exceptions list on page 206.

Procedure

1. On the client, double-click **My Network Places**.
2. In the My Network Places window, in the left pane, under the **Network Tasks** list, click **View Network Connections**.
3. In the Network Connections window, right-click the connection that you use to connect to the Internet and click **Properties**.
4. In the **<*connection*> Properties** dialog box, click the **Advanced** tab.
5. In the **Windows Firewall** section, click **Settings**.

   Important:

   If the Settings button is unavailable, Internet Connection Firewall is not enabled on this connection, and you cannot open any ports (because they are all already open).
6. In the **Windows Firewall** dialog box, click the **Exceptions** tab.
7. Click **Add Port** to open a new port.
8. In the **Add a port** dialog box, in the **Name** box, type `127.0.0.1`.

   You can specify the IP address of an internal computer, but you typically use 127.0.0.1.
9. In the **Port** number box, type the port number.
10. Select a communication option.
11. Click **OK**.
12. Repeat step 7 on page 207 to step 11 on page 207 for each port to open.
13. Click **OK** to close the **Windows Firewall** dialog box.
14. Click **OK** to close **<*connection*> Properties** dialog box.
15. Close the Network Connections window.

Variable definitions

Name	Description
<*connection*>	The connection that you use to connect to the Internet.

Name	Description
Communication options	The mechanism for communicating between the server and clients for reporting. TCP - Transmission Control Protocol UDP - User Datagram Protocol

Procedure job aid

If the client PC is running Windows XP Service Pack 2, open the following ports:

- Emergency Help: UDP 8200
- Multicast real-time reports: UDP 7020; 7030; 7040; 7050; 7060; 7070; 7080; 7090; 7100; 7110; 7120; 7130
- Unicast real-time reports: UDP 7025; 7035; 7045; 7055; 7065; 7075; 7085; 7095; 7105; 7115; 7125; 7135

Installing the ActiveX Controls

Before you begin

- Configure the Web browser to enable initialize and script ActiveX Controls not marked as safe. See Configuring Internet Explorer on page 203.

About this task

Install the ActiveX Controls.msi file on each client as an administrator if your company security policy prevents agents from logging on to clients as administrator.

The ActiveX controls are rules that specify how applications share information using the Web browser. In Contact Center, ActiveX controls allow communication between the clients and servers to report data and display information from the database.

Controls downloaded using the ActiveX Controls.msi file do not appear in the Internet Explorer Downloaded Program Files window.

Procedure

1. Log on to the client PC with administrator privileges.
2. Insert the Contact Center Installation DVD into the client, and navigate to **x:\\Install Software\CCMA\ActiveX Controls_<*patchID*>**; <*x*> is the drive letter of your DVD drive and <*patchID*> is the ID of the selected patch installed on the Contact Center Manager Administration server.
3. In the this directory, double-click **ActiveX Controls.msi** to begin the installation.
4. Click **Next**.

5. Select a **Destination Folder** or accept the default installation folder.
6. Click **Next**.
7. In the **Ready to Install the Program** window, click **Install**.
8. Click **Finish**.
9. Repeat steps 2 to 8 for each client.

Applying the ActiveX Controls

Before you begin

- Install the ActiveX.msi controls on your client. See Installing the ActiveX Controls on page 208.
- Ensure that you have administrator privileges to apply the ActiveX Controls.msi file to clients by using an SMS server or Group Policy.
- Configure the Web browser to enable initialize and script ActiveX Controls not marked as safe. See Configuring Internet Explorer on page 203.

About this task

Apply the ActiveX Controls.msi file you installed to the clients in your Contact Center to permit communication between the clients and servers in your network.

Because installation procedures performed through an SMS system can vary from one company to the next, this procedure offers general guidelines only.

In addition to using an SMS server, a system administrator can install this package on clients within the same domain using the Windows Group Policy.

For details, see the documentation on the Microsoft Web site at www.microsoft.com.

Procedure

1. Log on to the SMS server with administrator privileges.
2. Insert the Contact Center Manager installation DVD into the PC, and navigate to ***x*:\\Install Software\CCMA\ActiveX Controls_<*patchID*>** ; <*x*> is the drive letter of your DVD drive and <*patchID*> is the ID of the selected patch installed on the Contact Center Manager Administration server.
3. From the Contact Center Manager installation DVD, copy **ActiveX Controls.msi** to the desired directory on the SMS server.
4. Double-click **ActiveX Controls.msi** to run the installation and install the files on all SMS client PCs in your network.

Chapter 15: Communication Control Toolkit commissioning for SIP-enabled Contact Center

Use the procedures in this section to commission the Communication Control Toolkit (CCT) software in your SIP-enabled Contact Center.

Prerequisites to CCT commissioning for SIP-enabled Contact Center

- Read *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Complete *Avaya Aura® Contact Center Installation Checklist* (NN44400-310).
- Install all of the components required for the Communication Control Toolkit software for your network configuration, including the updates. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- Install Contact Center Manager Server if Communication Control Toolkit is installed for Avaya Aura® Contact Center. Contact Center Manager Server is not required if Communication Control Toolkit is installed for Knowledge Worker.
- Ensure the appropriate PABX is installed and configured for your system.
- Install CCT and all current updates.
- Install License Manager software and all current updates.
- Install and configure Contact Center Manager Server (CCMS) and Contact Center Manager Administration (CCMA).

Communication Control Toolkit commissioning for SIP-enabled Contact Center procedures

About this task

This task flow shows you the sequence of procedures you perform to commission the Communication Control Toolkit in a contact center environment.

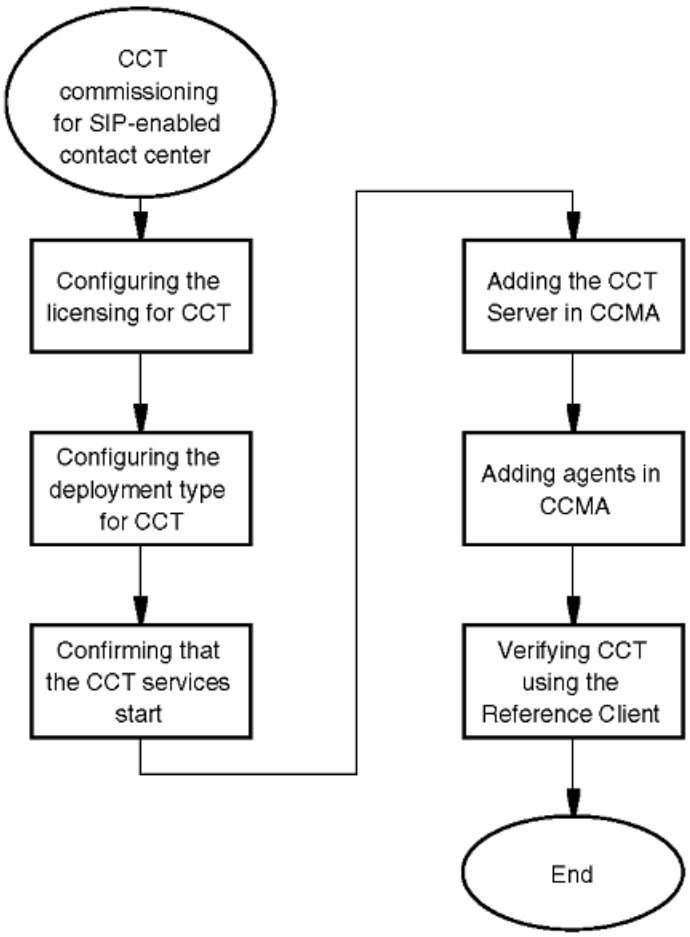


Figure 34: Communication Control Toolkit commissioning for SIP-enabled Contact Center procedures

Configuring the licensing for CCT

Before you begin

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

About this task

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

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

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

Procedure

1. Log on to the Communication Control Toolkit server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
3. Expand Communication Control Toolkit.
4. Expand **Server Configuration**.
5. Click **License Configuration**.
6. In 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.

   Important:

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

Variable definitions

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

Configuring the deployment type for CCT

Before you begin

- Understand the network requirements for your installation of CCT (co-resident, stand-alone, or multimedia).
- Know how to stop and restart the CCMS services. Stopping and restarting The Contact Center Manager Server services on page 496.
- Know how to stop and restart the CCT services. See Stopping and restarting the core Communication Control Toolkit services on page 495.

About this task

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.

Procedure

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

Variable definitions

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

Name	Description
	part of the solution and the OpenQ feature is disabled on the CCMS server.

Confirming that the CCT services start

About this task

Confirm that the Communication Control Toolkit services start so you can configure the Communication Control Toolkit database.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**.
2. Select the **CCT** tab.
3. Confirm that the Communication Control Toolkit services are running.
4. If a Communication Control Toolkit service is not running, re-start CCT.
5. Close the System Control and Monitor Utility.

Adding the CCT Server in CCMA

Before you begin

- To add a CCT server, you must first have added a CCMS with Open Queue enabled.
- Ensure you know the CCT Tomcat Web site port number. The default CCT Tomcat Web site port number is 8081.

About this task

Add the CCT server to CCMA then associate it to a CCMS server, to administer the CCT server from the CCMA client application. This is a summary of the full procedure outlined in *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

Procedure

1. Log on to Contact Center Manager Administration server.
2. On the Launchpad, click **Configuration**.

3. From the **Server** menu, click **Add Server**.
4. Enter details for the CCT server.
5. In the Associated CCMS Servers list, select the CCMS with which you want to associate this CCT server.
6. Click **Submit**.

Adding agents in CCMA for SIP-enabled Contact Centers

Before you begin

- Ensure all required windows users are created on the domain.
- Add CCT server to CCMA configuration, see Adding the CCT Server in CCMA on page 216.
- Log on to CCMA. For more information, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).
- Open the Contact Center Management component.

About this task

Create SIP agents using CCMA and associate them with contact center windows users. This is a brief summary of the procedure. For more details, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

Procedure

1. In the left pane, click the Contact Center Manager Server under which to add the agent.
2. From the **Add** menu, select **Agent**.
3. In the **New Agent Details** window, enter the mandatory information about the agent, login ID, Voice URI, Create CCT Agent, Primary Supervisor, Call Presentation and threshold.
4. Enter any optional information about the agent (for example, Title, Department, or Comments).
5. Select **Create CCT Agent**.
6. Click **Associate User Account**, and complete the Associate User Account fields to create a windows domain user for this agent.
7. Configure Multiplicity and Open Q if these features are enabled.
8. Configure the skillsets for the agent.

9. Click **Submit** to save your changes.

Verifying CCT using Reference Client

About this task

Verify Communication Control Toolkit configuration by using the Reference Client to ensure that all resources are available and accessible to route contacts for CCMS. The Reference Client is an installation testing tool and is not to be deployed for production contact center use.

Procedure

1. Log on to the Communication Control Toolkit server with the Local Administrator user ID and password.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **Ref Client**.
3. In the **Server Settings** dialog box, click **OK**.
4. From the **Session** menu, choose **Connect**.
5. In the **User Credentials** dialog box, enter the details of a user, enter a **User ID**, **Domain** and **Password**.
6. Click **OK**.
7. In the **Available Devices** box, select the address you want to use for the test call.
8. Enter the Destination Address in the text box to the right of the **Originate** button.
9. Click **Originate**. The destination address shows a Local State of Ringing in the Reference Client.
10. Select the Ringing Address on the Reference Client, and click **Answer**.
11. Release the call.

Chapter 16: Communication Control Toolkit commissioning for AML-based Contact Center

Use the procedures in this section to commission the Communication Control Toolkit (CCT) software in your AML-based Contact Center.

Prerequisites to CCT commissioning for AML-based Contact Center

- Read *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Complete *Avaya Aura® Contact Center Installation Checklist* (NN44400-310).
- Install all of the components required for the Communication Control Toolkit software for your network configuration, including the updates. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- Install Contact Center Manager Server if Communication Control Toolkit is installed for Avaya Aura® Contact Center. Contact Center Manager Server is not required if Communication Control Toolkit is installed for Knowledge Worker.
- Ensure the appropriate PABX is installed and configured for your system.
- Install CCT and all current updates.
- Install License Manager software and all current updates.
- Install and configure Contact Center Manager Server (CCMS) and Contact Center Manager Administration (CCMA).

Communication Control Toolkit commissioning for AML-based Contact Center procedures

About this task

This task flow shows you the sequence of procedures you perform to commission the Communication Control Toolkit in a contact center environment.

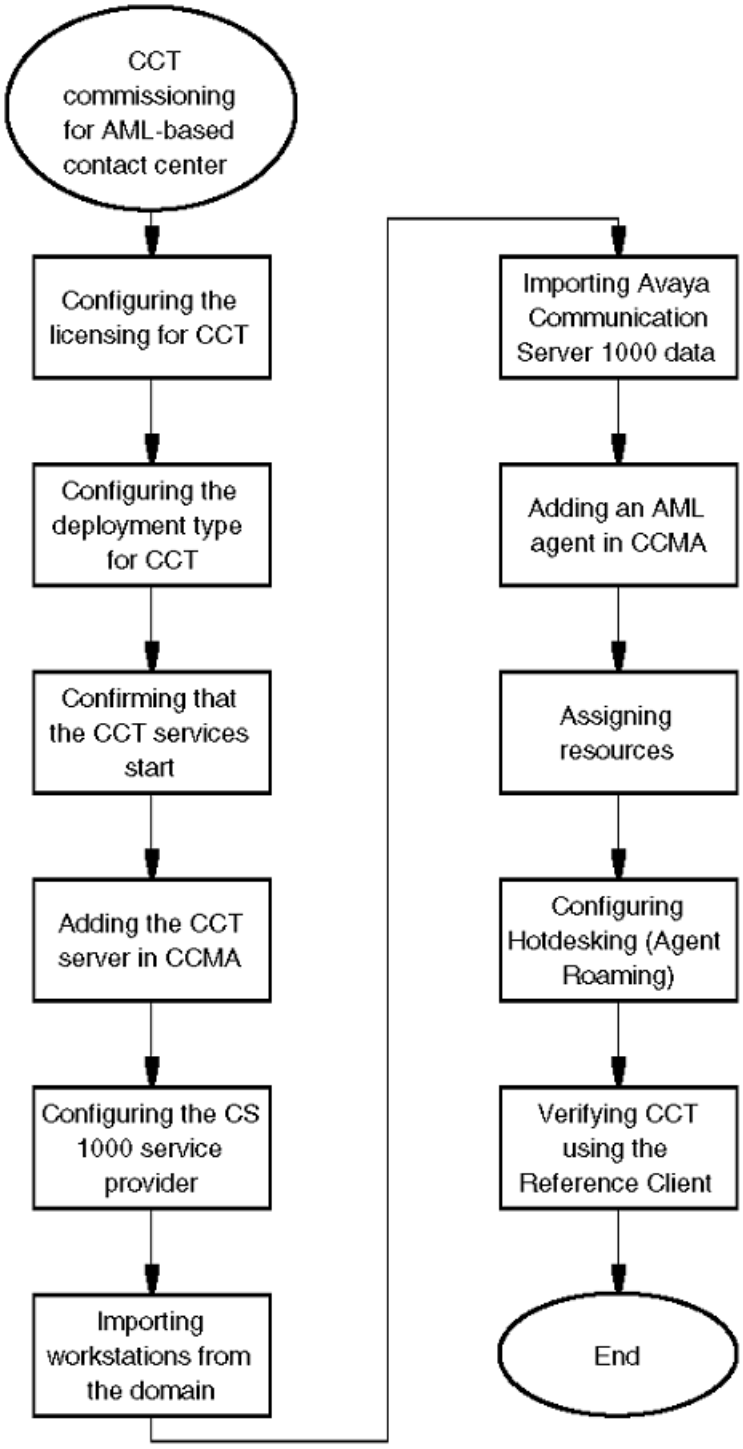


Figure 35: Communication Control Toolkit commissioning for AML-based Contact Center procedures

Configuring the licensing for CCT

Before you begin

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

About this task

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

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

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

Procedure

1. Log on to the Communication Control Toolkit server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
3. Expand Communication Control Toolkit.
4. Expand **Server Configuration**.
5. Click **License Configuration**.
6. In 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.

   Important:

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

Variable definitions

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

Configuring the deployment type for CCT

Before you begin

- Understand the network requirements for your installation of CCT (co-resident, stand-alone, or multimedia).
- Know how to stop and restart the CCMS services. Stopping and restarting The Contact Center Manager Server services on page 496.
- Know how to stop and restart the CCT services. See Stopping and restarting the core Communication Control Toolkit services on page 495.

About this task

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.

Procedure

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

Variable definitions

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

Name	Description
	part of the solution and the OpenQ feature is disabled on the CCMS server.

Confirming that the CCT services start

About this task

Confirm that the Communication Control Toolkit services start so you can configure the Communication Control Toolkit database.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**.
2. Select the **CCT** tab.
3. Confirm that the Communication Control Toolkit services are running.
4. If a Communication Control Toolkit service is not running, re-start CCT.
5. Close the System Control and Monitor Utility.

Adding the CCT Server in CCMA

Before you begin

- To add a CCT server, you must first have added a CCMS with Open Queue enabled.
- Ensure you know the CCT Tomcat Web site port number. The default CCT Tomcat Web site port number is 8081.

About this task

Add the CCT server to CCMA then associate it to a CCMS server, to administer the CCT server from the CCMA client application. This is a summary of the full procedure outlined in *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

Procedure

1. Log on to Contact Center Manager Administration server.
2. On the Launchpad, click **Configuration**.

3. From the **Server** menu, click **Add Server**.
4. Enter details for the CCT server.
5. In the Associated CCMS Servers list, select the CCMS with which you want to associate this CCT server.
6. Click **Submit**.

Configuring the Avaya Communication Server 1000 service provider

Before you begin

- Understand the server provider details for the switch.

About this task

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 to the PABX. The polling interval detail is configured in the Avaya Communication Server 1000 service provider details. The default polling time is ten seconds.

Procedure

1. Log on to Contact Center Manager Administration server.
2. Start Communication Control Toolkit Web Administration client.
3. In the resource menu, select **Providers**.
   The details of the providers appear.
4. From the list of providers, select **Passive**.
5. In the **Basic Provider Information** section, in the **Passive Name** box, type the Provider name.

   Important:

   The provider name must be Passive.
6. In the **IP Address** box, type the IP address of the provider.
7. In the **Port** box, type the port number.
8. In the **Provider Configuration** section, from the **Transport** list, select **TCP**.
9. In the **Customer Number** box, type the customer number.

10. From the **CS1000 Software Release** list, select the software release of your Avaya Communication Server 1000.
11. In the **Call Data Life Span (minutes)** box, type the required value in minutes.
12. Select or clear the **Disable Copy of Data to Consult Call** check box.
13. In the **CS1000 Home location Code (HLOC)** box, type the HLOC value.
14. In the **Network IVR Port** box, type the port value.
15. In the **Initialization Timeout (seconds)** box, type the **Initialization timeout** setting in seconds.
16. In the **Command Timeout (seconds)** box, type the **Command** timeout setting in seconds.
17. Select **Save**.

Variable definitions

Name	Description
Provider Name	Name of the Provider, Passive.
IP Address	In a Contact Center environment, the IP address of the CCMS.
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.
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 Avaya 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.

Name	Description
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.

Importing workstations from the domain

Before you begin

- A local administrator must have access to the contact center domain to import domain resources to the CCT Console. Ensure the local administrator has access to the contact center domain.

About this task

All Contact Center applications are in a contact center domain. Import workstations from the contact center domain to the Communication Control Toolkit server using the Import Workstations tool.

Procedure

1. Log on to the Communication Control Toolkit server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
3. Expand Communication Control Toolkit.
4. Click **Import Work Stations**.
5. From the **Search Type** list, select **All WorkStations**.
6. Select the workstations to import from the **Available Work Stations** list.
7. Click **Add**.

8. Click **OK**.

Importing Avaya Communication Server 1000 data

Before you begin

- Connect a COM cable from a server (not the Communication Control Toolkit server) or workstation to the switch.
- Know the user ID and password to log on to the Avaya Communication Server 1000.
- Apply all Avaya Communication Server 1000 patches, specifically patch MPLR26704. Patch MPLR26704 significantly reduces the time to import address and terminal information into the text file. Only information that is relevant to Communication Control Toolkit is imported.
- Only PABX keys that are AST and IAPG enabled are imported.

About this task

You can use the CCT Import CS 1000 Data tool to perform either of the following activities:

- Perform the first step of the import process: convert data capture text file to an XML file by un-checking the Automatically import data after conversion check box.
- 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.

You can convert the text file to an XML file to test the data import facility without modifying the database contents; or, you can postpone the actual import of the data to an off peak time. You can later import the intermediate XML data file generated by using the CCT Data Import/Export Tool, by selecting the Standard XML format option.

Before importing the Avaya Communication Server 1000 data to CCT, you must first retrieve the data from the switch. To do this, create a switch configuration text file to capture the Avaya Communication Server 1000 data required to configure Communication Control Toolkit.

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

Procedure

1. Open a text editor on the server on which 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 the user ID and password for the switch.
15. If the prompt does not appear, continue to press **Enter** until the prompt appears.
16. Browse to the download.txt file, and then click **Start**.
17. Type these commands at the following prompts:

```
>LD 20
REQ: PRT
TN: TNB
TN: Press enter
CDEN: Press enter
CUST: 0 (or the customer number)
DATE: Press enter
PAGE: ON
DES: Press enter
```

    Downloading information from the Avaya Communication Server 1000 overlay can take a several minutes.

18. To return to the prompt, enter ******** (Shift + 8888).
19. Press **Enter**.
20. Type these commands at the following prompts:

```
>LD 23
REQ: PRT
TYPE: CDN
CUST: 0 (or the customer number)
CDN: Press enter
```

    The information is downloaded from the overlays.

21. Type **logo**.
22. Press **Enter**.
23. Copy the download.txt to the Communication Control Toolkit server.

24. Log on to the Communication Control Toolkit server.
25. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
26. Expand Communication Control Toolkit.
27. Expand **Bulk Provisioning**.
28. Select **Import CS 1000 Data**.
29. Select **Passive** for the Avaya Communication Server 1000 Provider.
30. Select **Input File**. This opens a file explorer to select the Avaya Communication Server 1000 data capture file you copied in step 23 on page 230.
31. Select the Avaya Communication Server 1000 data capture file, click **Open**. A default path and file name appears in the **Output file**, change the location if necessary.
32. To import the data into the database select **Automatically import data after conversion**.
33. In the Actions pane on the right hand side, select **Convert/Import**. A progress bar in the Status area indicates the progress made by the tool in three phases:
    - Conversion of the data capture file
    - Generation of the output file
    - Import of the data into the database
34. The status area displays data imported and the conversion results, including the number of TNs, DNs, and CDNs found. If applicable, a list of errors are also displayed. This list includes line numbers where the errors were discovered in the supplied data capture file.

    Important:

    An error dialog shows errors in the conversion step. The error dialog appears prior to beginning the automatic import. The user can choose to cancel the import step or proceed.

Adding an AML agent in CCMA

Before you begin

- If you have a CCT server in the contact center, ensure that you have a domain user account for your contact center domain with privileges to list the domain users.
- Add CCT server to CCMA configuration.

- Log on to CCMA. For more information, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).
- Open the Contact Center Management component.

About this task

Create AML agents on the CCMA server and associate them with the appropriate contact center windows users. Use this procedure to add one agent to your Contact Center for testing purposes. To add multiple agents, see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

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

Procedure

1. In the left pane, click the Contact Center Manager Server under which to add the agent.
2. From the **Add** menu, select **Agent**.
3. In the New Agent Details window, enter the mandatory information about the agent, First Name, Last Name, Login ID, Create CCT Agent, Primary Supervisor, Call Presentation and threshold.
4. Enter any optional information about the agent (for example, Title, Department, or Comments).
5. Select **Create CCT Agent**.
6. Click **Associate User Account**, and complete the Associate User Account fields to create a CCT user for this agent.
7. Configure the Skillsets for the agent.
8. Click **Submit** to save your changes.

Assigning resources in Contact Center

About this task

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 stores 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

1. Log on to Contact Center Manager Administration server.
2. Start the **Communication Control Toolkit Web Administration**.
3. Click the resource type.
4. Click the single resource to configure.
5. Select one of the Resource Assignments to assign to this resource.
6. 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 clear it.
7. Click **the Right Arrow** to move the selected resource and resource groups to the **Assigned Resources** column.
8. Click **Save**.

Example of assigning resources

About this task

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.

Procedure

1. Log on to the CCMA server.
2. Start the **Communication Control Toolkit Web Administration** client.
3. Select **Groups**.
4. Select **Terminal Groups**.
5. Select the hotdesking_terminals terminal group.
6. Select the all terminals in the **Available Resources** column.

Click each resource to select more than one resource.

7. Click **the Right Arrow** to move the selected terminals to the **Assigned Resources** column.
8. Click **Save**.

Configuring Hotdesking (Agent Roaming)

Before you begin

- 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 a correctly mapped address.
- 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.

About this task

In a contact center an agent may not have a fixed desk and phone. An agent may pick a desk that is not being used and log into the phone and workstation. An agent must be able to log on to any phone and workstation in this environment.

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.

Procedure

1. Place all select terminals for hotdesking into a terminal group.
2. Ensure that all terminals have a correctly mapped address.
3. Place all the addresses associated with the terminals into an address group.

Comments? infodev@avaya.com

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.

Important:

You can assign a terminal to only one workstation.

Verifying CCT using the Reference Client

Before you begin

- Create a Windows user for testing.
- Configure CCT for your contact center.

About this task

Verify Communication Control Toolkit configuration by using the Reference Client to ensure that all resources are available and accessible to route contacts for CCMS. The Reference Client is an installation testing tool; do not deploy it for production contact center use.

Procedure

1. Log on to the Communication Control Toolkit server with the Local Administrator user ID and password.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **Ref Client**.
3. In the **Server Settings** dialog box, click **OK**.
4. From the **Session** menu, choose **Connect**.
5. In the **User Credentials** dialog box, select either the **Current Windows User** or specify a **User ID**, **Domain** and **Password**.
6. Click **OK**.
7. In the **Available Devices** box, select the address you want to use for the test call.
8. Enter the Destination Address in the text box to the right of the Originate button.
9. Click **Originate**. The destination address shows a Local State of Ringing in the Reference Client
10. Select the Ringing Address on the Reference Client, and click **Answer**.

11. Release the call.

Chapter 17: Contact Center Multimedia server commissioning

Commission the Contact Center Multimedia server to manage multimedia contacts in your Avaya Aura® Contact Center.

Contact Center Multimedia server commissioning prerequisites

About this task

- Install Contact Center Manager Server in the Contact Center. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Install Contact Center Manager Administration server software in the Contact Center. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Install Communication Control Toolkit server software in your Contact Center. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Install Contact Center Multimedia server software in your Contact Center. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Configure Open Queue as a feature in the Contact Center Manager Server installation. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Configure Communication Control Toolkit on the Contact Center Manager Server configuration window. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Commission the Communication Control Toolkit server. See Communication Control Toolkit commissioning for SIP-enabled Contact Center on page 211 or Communication Control Toolkit commissioning for AML-based Contact Center on page 219.
- Apply the most recent service packs for Contact Center Multimedia. See *Avaya Aura® Contact Center Upgrade and Patches* (NN44400-410).

Contact Center Multimedia server commissioning procedures

About this task

To commission the Contact Center Multimedia server, you must perform the following procedures.

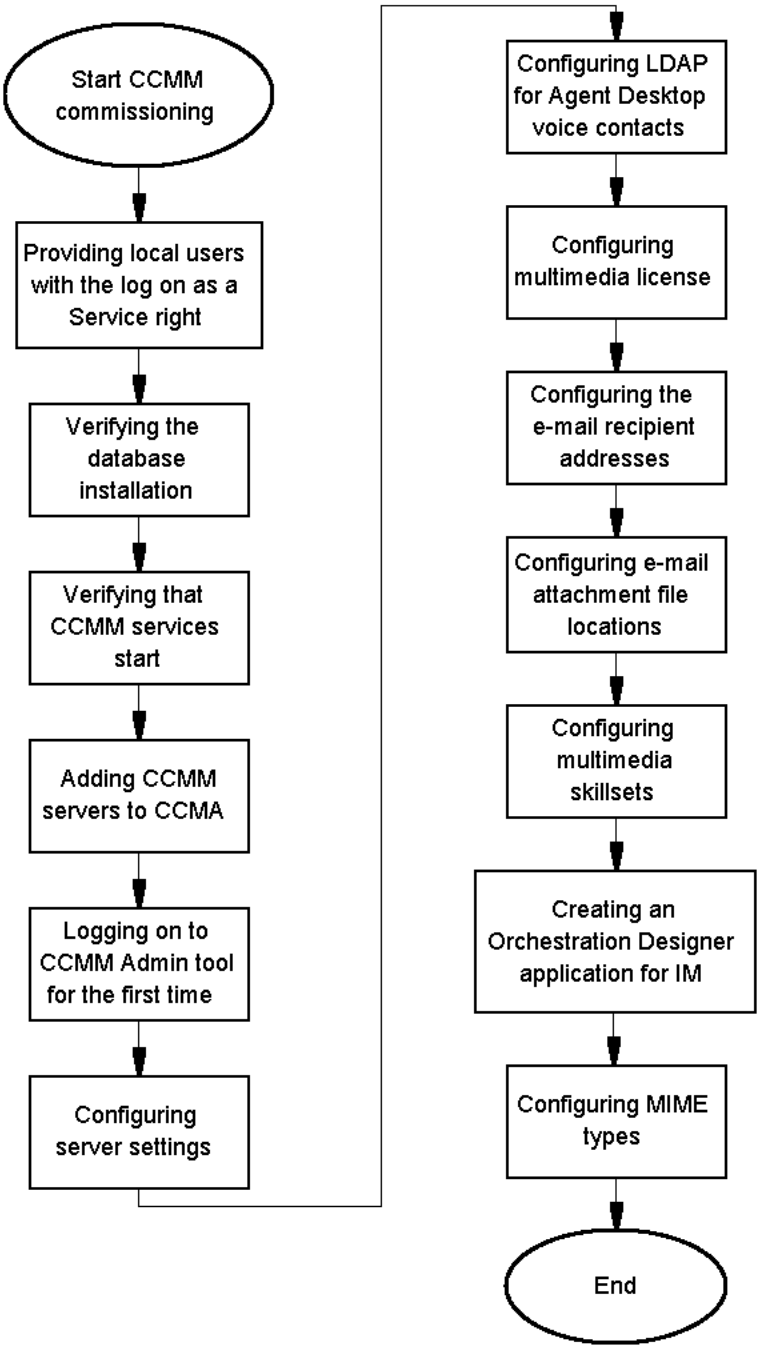


Figure 36: Contact Center Multimedia server commissioning procedures

Job aid: Timing

The estimated time to commission Contact Center Multimedia is 1 hour.

Providing local users with the Log on as a service right

About this task

Provide local users with the log on as a service right to ensure that administrators and the agents in your Contact Center have access to the Contact Center Agent Desktop application.

Procedure

1. Click **Start** > **Administrative Tools** > **Local Security Policy**.
2. Under **Security Settings**, in the left pane, double-click **Local Policies**.
3. In the left pane, click **User Rights Assignment**.
4. In the right pane, double-click **Log on as a service**.
5. Click **Add User or Group**.
6. Click **Locations**.
7. In the **Locations** dialog box, select the Contact Center Multimedia server name from the list.
8. Click **OK**.
9. In the **Enter the object name to select** box, type **IUSR**.
10. Click **Check Names** to verify that the user name exists on the local computer.
11. Click **OK**.
12. Click **Apply** to save the changes.
13. Click **OK**.
14. Close the **Local Security Settings** window.

Variable definitions

Name	Description
IUSR	An Internet Information Services (IIS) account used for all communication between the Multimedia server and the Contact Center Agent Desktop over HTTP.

Verifying the Multimedia database installation

Before you begin

- Install Contact Center Multimedia.
- Log on to the Contact Center Multimedia server.

About this task

Verify that the Multimedia database is installed and configured correctly.

Procedure

1. On the Contact Center Multimedia server, open Internet Explorer.
2. Browse to **http://<servername>/csp/multimedia/ws.Contact.cls**, where <servername> is the name of the Contact Center Multimedia server.
3. If a Web page does not appear, contact your Avaya technical support prime.

Verifying that Contact Center Multimedia services start

Before you begin

- Log on to the Contact Center Multimedia server.

About this task

Verify that Contact Center Multimedia services start to ensure that contacts are routed immediately after the server restarts for any reason.

Procedure

1. On the Contact Center Multimedia server, click **Start** > **Administrative Tools** > **Services**.
2. Next to **CCMM License Service**, verify that the status is **Started** and the startup type is **Automatic**.
3. Next to **CCMM Starter Service**, verify that the status is **Started** and the startup type is **Automatic**.
4. Verify that the following services started:
   - CCMM Multimedia Contact Manager
   - CCMM OAM service
   - CCMM Campaign Scheduler service
5. If the contact center has licenses for e-mail or predictive outbound contacts, verify that the following services started:
   - CCMM Email Manager
   - CCMM Predictive Outbound Blending
   - CCMM Predictive Outbound Service
6. If any service does not start, in the Services window, right-click the service name, and then click **Start**.

Adding the multimedia servers to Contact Center Manager Administration

Before you begin

- Obtain a user ID and password for the Contact Center Manager Administration client application.
- Know the computer name of the server to add.

About this task

Add the servers necessary to manage multimedia contacts to the Contact Center Manager Administration to provide reporting and connectivity support.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Log on to Contact Center Manager Administration.

3. On the Launchpad, click **Configuration**.
4. On the configuration menu, select **Server** > **Add Server**.
5. From the **Type** list, select CCMM.
6. In the **Server Name** box, type the computer name of the Multimedia or Predictive Outbound server.
7. Press the Tab key.
   The server IP address automatically appears in the IP Address box.
8. In the **Display Name** box, type the name of the Multimedia or Predictive Outbound server as you want it to appear in the system tree in Contact Center Manager Administration.

   The system automatically assigns a display name that is the same as the server name. To enter a different display name, you must enter a unique name.
9. To add a Contact Center Multimedia server, in the **Login ID** box, type `mmReport`.
10. In the **Password** box, type your password

    Important:

    You must change this password if the system sends a message that contains a logon request for validation.
11. Click **Submit**.
12. Click the plus symbol (+) beside the server name to access the server.
13. In the left pane, select the Contact Center Manager Server with which you want to associate the Contact Center Multimedia server.
14. Right-click the Contact Center Manager Server and then click **Edit Properties**.
15. Under **Associated Reporting Server**, select the check box next to the current active Contact Center Multimedia server name.
16. Click **Submit**.

Variable definitions

Name	Description
Login ID	For Contact Center Multimedia, the Login ID corresponds to the user in running historical reports in Contact Center Manager Administration. This user is configured in the Multimedia database and has access to data

Name	Description
	within that database. The Login ID is always mmReport.
Password	For Contact Center Multimedia, the default password is mmRep. To change this password, use the Contact Center Multimedia Administrator.

Logging on to the Multimedia Administration tool for the first time

Before you begin

- Obtain a user ID and password for the Contact Center Manager Administration client application.

About this task

Log on to the Contact Center Multimedia Administration tool to configure the Contact Center.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Start Internet Explorer.
3. In Internet Explorer, choose **Tools** > **Internet Options** > **Trusted Sites** > **Custom Level**.
4. Under **Downloads**, for **Automatic prompting for file downloads**, select **Enable**.
5. In Internet Explorer, choose **Tools** > **Internet Options** > **Security** > **Trusted Sites** > **Sites**.
6. Under **Add this website to the zone**, type the name of the CCMM server.
7. Click **Close**.
8. Click **OK**.
9. Log on to the Contact Center Manager Administration client with administrative privileges.
10. On the **Launchpad**, click **Multimedia**.
11. In the left pane, select the Contact Center Multimedia server to which you want to log on.
12. Select **Install Prerequisite Software**, and click **Launch Multimedia Client**.

13. On the Internet Explorer window, click **Run**.
    The Contact Center Multimedia Administration tool appears.

Configuring server settings

Before you begin

- Ensure that you understand for which contact types your Contact Center is licensed.
- Install the required software on your Web server and E-mail servers (if applicable).

About this task

Configure the Contact Center application servers, Web communications, and e-mail servers to ensure that you can connect the Contact Center Multimedia server to the external servers for handling e-mail, voice mail, fax, scanned documents, and Web communications contacts.

Certain server types appear by default because the install required the details for these servers. Additionally you can add the following server types:

- CallPilot Server
- Communication Manager Server
- Communication Manager Standby Server
- Geographic Alternate CCT Server
- Inbound POP3 Server
- Outbound SMTP Server
- Secondary Predictive Application Server
- TSP Dialer

Important:

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

Procedure

1. Log on to Contact Center Manager Administration with administrator privileges.
2. On the Launchpad, click **Multimedia**.
3. In the left column, select the Multimedia server on which you want to configure server settings.
4. In the left column, select **General Administration**.
5. Click **Server Settings**.

6. Select the server to update, and click **Edit**.
7. In **Edit Server**, type the details for the server.
8. Click **Save**.

Variable definitions

Name	Description
Server Name	The host name of the server.
Server Port	The communications port number for the server.
Server Type	Choose the server type, for example; CCT, CCMS, License Manager, or Standby CCT.
Backup Server	The standby license server name.
MCMC Event Port	The Multimedia Contact Management Client port number.
Primary Hostname	The host name of the primary e-mail server. Required for Outbound SMTP and Inbound POP3 server types.
Port Number	The server port that CCMM uses to communicate with the server. Required for Outbound SMTP, Inbound POP3, Secondary Predictive Application, and Geographic Alternate CCT server types.
Secondary Hostname	The host name of the optional secondary e-mail server. Available for Outbound SMTP and Inbound POP3 server types.
SMTP Authentication	Enable or disable SMTP Authentication. Required for Outbound SMTP Server.
Username	The LDAP Server access account name. Required for Directory LDAP and Phonebook LDAP server types.
Password	The LDAP Server access account password.Required for Directory LDAP and Phonebook LDAP server types.
Search base	The LDAP base search string. Required for Directory LDAP and Phonebook LDAP server types.

Name	Description
Polling Interval (hrs)	The LDAP polling interval. Required for Directory LDAP and Phonebook LDAP server types.

Configuring an LDAP server for Agent Desktop voice contacts

Before you begin

- Ensure that the LDAP server that you use for voice contacts is commissioned and operational.

Important:

To retrieve contacts from the LDAP server, ensure that the Enable Address Book Retrieval check box is selected.

About this task

Configuring an Lightweight Directory Access Protocol (LDAP) server provides agents using Agent Desktop with a list of contacts during a voice call.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Open the Contact Center Manager Administration application.
3. Type your user ID and password.
4. Click **Multimedia**.
5. In the left column, select **General Administration**.
6. Click **Server Settings**.
7. Click **New** and select the **Phonebook LDAP** option.
   The Phonebook LDAP Server Configuration dialog box appears.
8. Click **Edit Server** and type the server name.
9. Add the LDAP information.
10. Click **Test** to test the username, password and search base, by connecting to the configured server to retrieve contacts.
11. Click **Save**.

Variable definitions

Name	Description
Server Name	The host name of the server.
Server Port	The communications port number for the server.
Server Type	The server type, for example; CCT, CCMS, License Manager, or Standby CCT.
Enable Address Book Retrieval	To retrieve contacts from the LDAP server, ensure that the Enable Address Book Retrieval check box is selected. This check box is selected by default.
Username	The LDAP Server access account name. Username must be in the format <*domainname*>\<*username*> (for example, europe\adminuser) or <*username*>@<*domainname*> (for example, adminuser@europe.com).
Password	The LDAP Server access account password.
Search base	The LDAP base search string.
Polling Interval (hrs)	The LDAP polling interval.

Configuring the multimedia license type

About this task

Configure the license type for the Contact Center Multimedia server. The license you choose must match the system license purchased for your contact center.

Nodal licensing is for single sites of Contact Center; corporate licensing enables multiple sites.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Open the Contact Center Manager Administration application.
3. Type your user ID and password.
4. On the **Launchpad**, click **Multimedia**.

The system opens the CCMM Administration application.

5. In the left column, click **General Administration**.
6. Click **General Settings**.
7. Under **License Type**, select the type of license used in your contact center.
8. Under **RTD Multicast Configuration**, in the **Multicast IP** box, type the Multicast send IP address from Contact Center Manager Server.
9. Under **RTD Multicast Configuration**, in the **Port** box, type the skillset port number from Contact Center Manager Server.
10. Click **Save**.

Configuring e-mail recipient addresses

Before you begin

- Ensure that you understand for which contact types your Contact Center is licensed.

About this task

Configure the recipients in your contact center to handle e-mail, voice mail, fax, scanned documents, and SMS contacts. Each type of contact is scanned and attached to an e-mail that is received by the contact center and routed. You must configure the recipient mailboxes to ensure the contacts are routed.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Open the Contact Center Manager Administration application.
3. Type your user ID and password.
4. On the **Launchpad**, click **Multimedia**.
   The system opens the CCMM Administration application.
5. In the left column, select **Email**.
6. Click **Recipient Addresses**.
7. Click **New**.
8. From the **Mailbox Type** list, select **Mail Store** or **Alias**.
9. Enter the mailbox details.
10. Click **Save**.

Variable definitions

Name	Description
Display name	The name to appear in the e-mail From address.
E-mail Domain	The domain for your e-mail server.
Mail Store or Alias	Select the Mail Store or Alias option. • Select Mail Store to include the e-mail mailbox in the set of mailboxes from which incoming e-mail is retrieved. • Select Alias to configure this mailbox as an alias. The address of an alias can be used in rules configuration and outbox mapping, but a recipient box configured as an alias address not contain e-mail.
Mailbox Name	The name of the mailbox that receives incoming e-mail to the Contact Center. If the Contact Center Multimedia server is not in the same domain as the e-mail server, you must also include the domain. Include the domain in the format domain\user (Windows 2000) or user@domain (post- Windows 2000) in the Mailbox Name box. Example: To enter the e-mail address `sales@avaya.com`, in the Mailbox Name box, type sales, and in the E-mail Domain box, type avaya.com. Example: To enter the e-mail address `sales@europe.avaya.com`, in the Mailbox Name box, type europe\sales or `sales@europe.avaya.com`, and in the E-mail Domain box, type europe.avaya.com.
Password Confirm	The password for your mailbox. When you change a password on the e-mail server, you must update this password in the Multimedia Administrator.
POP3 Server	The name of the mail server that handles the e-mail into the Contact Center.
Inbound Mail Threshold	The maximum number of e-mail messages the mailbox can accept every time it scans the database. You can enter a different value

Name	Description
	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.
SMTP Server	The name of the mail server that handles the e-mail that leaves the Contact Center.
Use alternative user name for SMTP Authentication	Select this box if you are configure an inbox as an alias. If SMTP authentication is enabled on your E-mail Server, and you use aliases, you log on to the SMTP server with a different user name.
Username	The logon name for the SMTP server. You can have mailboxes on multiple e-mail servers. You can have multiple e-mail servers for e-mail or fax messages, load balancing, and managing e-mail subtypes. Each e-mail server is polled for the mailboxes that it hosts. Configure additional e-mail servers using the Server Configuration window. For instructions about configuring additional e-mail servers, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

Configuring e-mail attachment file locations

About this task

Configure the locations for inbound and outbound e-mail attachments.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Open the Contact Center Manager Administration application.
3. Type your user ID and password.
4. On the **Launchpad**, click **Multimedia**.
   The system opens the CCMM Administration application.
5. In the left column, select **E-mail**.
6. Click **General Settings**.

7. Under **Attachment Files**, in the **Inbound URL** box, type the URL for files attached to inbound e-mail messages.
8. Under **Attachment Files**, in the **Inbound Share** box, type the share location for files attached to inbound e-mail messages.
9. Under **Attachment Files**, in the **Outbound URL** box, type the URL for files attached to outbound e-mail messages.
10. Under **Attachment Files**, in the **Outbound Share** box, type the share location for files attached to outbound e-mail messages.
11. Click **Save**.

Variable definitions

Name	Description
Inbound URL	The URL for files attached to inbound e-mail messages. For contact centers using the Avaya Aura® Contact Center High Availability feature, Avaya recommends using: http://<managedIPAddress>/InboundAttachment Where managedIPAddress is the managed IP address of the CCMM server.
Inbound Share	The share location for files attached to inbound e-mail messages. Avaya recommends using: <driveLetter>:\Avaya\Contact Center\Email Attachments\Inbound
Outbound URL	The URL for files attached to outbound e-mail messages. For contact centers using the Avaya Aura® Contact Center High Availability feature, Avaya recommends using: http://<managedIPAddress>/OutboundAttachment Where managedIPAddress is the managed IP address of the CCMM server.
Outbound Share	The share location for files attached to outbound e-mail messages. Avaya recommends using: <driveLetter>:\Avaya\Contact Center\Email Attachments\Outbound

Configuring the multimedia skillsets

Before you begin

- Ensure that you understand for which contact types your Contact Center is licensed.
- Configure the route points in Contact Center Manager Administration that you plan to use for the multimedia skillsets.

About this task

Configure multimedia skillsets to ensure that you can route multimedia contacts in your contact center. Multimedia contacts include e-mail, fax, scanned documents, SMS text messages, voice mail, Web communications, and outbound contacts. Instant messages are manually scripted in Orchestration Designer. For more information about instant messaging configuration, see Creating an Orchestration Designer application to route from an IM route point to an IM skillset on page 254.

You must configure a route point for each default skillset, and add any other skillset you intend to use for routing contacts.

Procedure

1. Log on to the Contact Center Manager Administration server.
2. Open the Contact Center Manager Administration application.
3. Type your user ID and password.
4. Click **Multimedia**.
5. In the left column, select **General Administration**.
6. Click **Skillset Settings**.
7. Select the skillset to update, and click **Edit**.

   Important:

   You must configure at least one skillset for each type of contact for which your contact center is licensed. You must configure the default skillset.
8. In the **Route Point** box, select a Route Point for the skillset.
9. Repeat step 7 on page 253 and step 8 on page 253 for each default skillset.

Variable definitions

Name	Description
Route Point	An equivalent routing number for a non voice contact. You must configure Route points in Contact Center Manager Administration.
Skillsets	You must configure at least one skillset for each contact type for which you are licensed. • E-mail skillsets are prefixed by EM_. You can also configure an optional automatic response for an e-mail skillset that is used to respond immediately to an e-mail message from a customer. • Outbound skillsets are prefixed with OB_. • Web Communication skillsets are prefixed with WC_. • SMS text message skillsets are prefixed with SM_. • Instant Message skillsets are prefixed with IM_. • Voice mail skillsets are prefixed with VM_. • Fax skillsets are prefixed with FX_. • Scanned document skillsets are prefixed with SD_.

Creating an Orchestration Designer application to route from an IM route point to an IM skillset

Before you begin

- You are familiar with creating and editing flows in Orchestration Designer. See *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (NN44400-510).
- You have access to an Orchestration Designer client and privileges to create flows for this contact center.

About this task

Create an application in Orchestration Designer to route IM contacts from the IM route point to an IM skillset.

Procedure

1. In Orchestration Designer, create a new flow to route IM contacts.
2. Edit the flow elements to route IM contacts received on the IM route point to an IM skillset.

Configuring the MIME types

Before you begin

- Install Contact Center Multimedia server software.
- Log on to the Contact Center Multimedia server.

About this task

Configure the Multipurpose Internet Mail Extension (MIME) types to ensure that agents can access e-mail message attachments.

Procedure

1. From the **Start** menu of the Contact Center Multimedia server, click **Administrative Tools** > **Computer Management**.
2. In the **Computer Management** dialog box, expand **Services and Applications** > **Internet Information Services** > **Sites**.
3. Select **Default Web Site**.
4. Under **IIS**, select **MIME Types**.
5. Double-click **MIME Types**.
6. On the **Actions** list on the right, click **Add**.
7. In the **File name extension** box, type `.dic`.
8. In the **MIME Type** box, type `application/octet-stream`.
9. Click **OK**.
10. On the **Actions** list on the right, click **Add**.
11. In the **File name extension** box, type `.eml`.
12. In the **MIME Type** box, type `application/octet-stream`.

13. Click **OK**.
14. On the **Actions** list on the right, click **Add**.
15. In the **File name extension** box, type `.dat`.
16. In the **MIME Type** box, type `application/octet-stream`.
17. Click **OK**.
18. Close the Computer Management window.

Variable definitions

Name	Description
Extension	The Multipurpose Internet Mail Extension (MIME) types required by Avaya Aura® Agent Desktop. • .dic • .eml • .dat
MIME Type	The Multipurpose Internet Mail Extension (MIME) information required by Avaya Aura® Agent Desktop: application/octet-stream.

Chapter 18: Agent Desktop client commissioning

Commission each Avaya Aura® Agent Desktop client in your Avaya Aura® Contact Center to run the Avaya Aura® Agent Desktop application.

Prerequisites for Agent Desktop client commissioning

- Install Contact Center Multimedia or Agent Desktop. See *Avaya Aura® Contact Center Installation* (NN44400-311).

Agent Desktop client communications server commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to commission or set up the Agent Desktop clients.

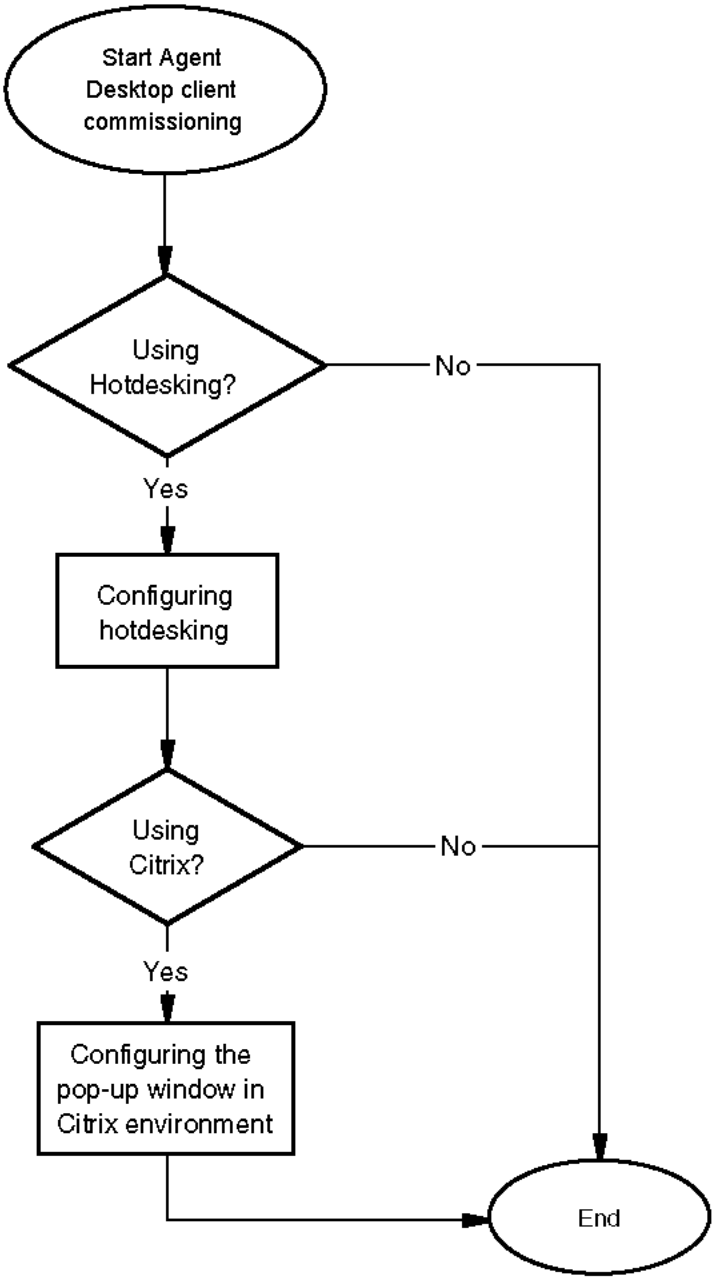


Figure 37: Avaya Aura® Agent Desktop client commissioning procedures

Configuring hotdesking (optional)

Before you begin

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

About this task

Configure hotdesking in your Contact Center so that an agent can sit at any desk and log on to the Agent Desktop.

With hotdesking enabled and configured, when agents start the Agent Desktop, they automatically map to the relevant terminal and addresses without user intervention.

If you use a Citrix environment, you must configure the prompt for the workstation. For more information, see Configuring the pop-up window for a Citrix environment on page 259.

Procedure

1. Select the CCMM server, and start the CCMM administration utility.
2. In the left column, select the Multimedia server on which you want to configure agent hotdesking.
3. In the left column, select **Agent Desktop Configuration**.
4. Choose **General Settings**.
5. Under **Hot Desking**, select the **Enabled** check box.

Configuring the pop-up window for a Citrix environment

Before you begin

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

About this task

Configure the pop-up window to allow agents to log on to their computer using their own user ID and password in a Citrix environment.

Procedure

1. Click **Multimedia**.
2. In the left column, select the Multimedia server on which you want to configure the pop-up window.
3. In the left column, select **Agent Desktop Configuration**.
4. Choose **General Settings**.
5. Under **Hot Desking**, select the **Prompt for Workstation** check box.

Chapter 19: Agent Greeting commissioning

The Agent Greeting feature allows agents to record personal greetings that the system can play automatically when an agent answers a voice contact. Agents can also record time of the day greetings (if the administrator has configured the Time of Day settings). Only SIP-enabled contact centers support Agent Greeting.

The procedures in this taskflow vary depending on the SIP Voice proxy of your PABX. The following PABXs use the specified proxies:

- Avaya Aura® 6.1, Avaya Aura® 6.2, and Avaya Communication Server 1000 Release 7.5 use Session Manager
- Avaya Communication Server 1000 Releases 7.0 and earlier use Network Routing Service (NRS)
- Avaya Aura® Unified Communications (Communication Manager or Midsize Business Template 5.2.1) uses SIP Enablement Services (SES)

Important:

If you delete an agent or supervisor using Contact Center Manager Administration, you can then use Avaya Media Server - Element Manager to delete their recorded greetings. Using Avaya Media Server - Element Manager to manipulate Agent Greeting prompts is not supported. Use Element Manager only to delete recorded greetings. Agent Greeting prompt manipulation is supported only when using the Agent Greeting telephony prompt menu.

Prerequisites for Agent Greeting commissioning

- Install and commission your SIP contact center including all Avaya MS configuration.
- Enable the Agent Greeting license on the Contact Center License Manager.

Agent Greeting commissioning procedures

About this task

This taskflow shows you the sequence of procedures you perform to commission Agent Greeting.

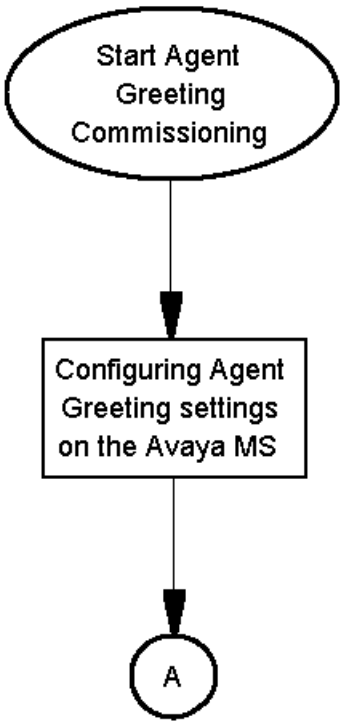


Figure 38: Agent Greeting commissioning navigation

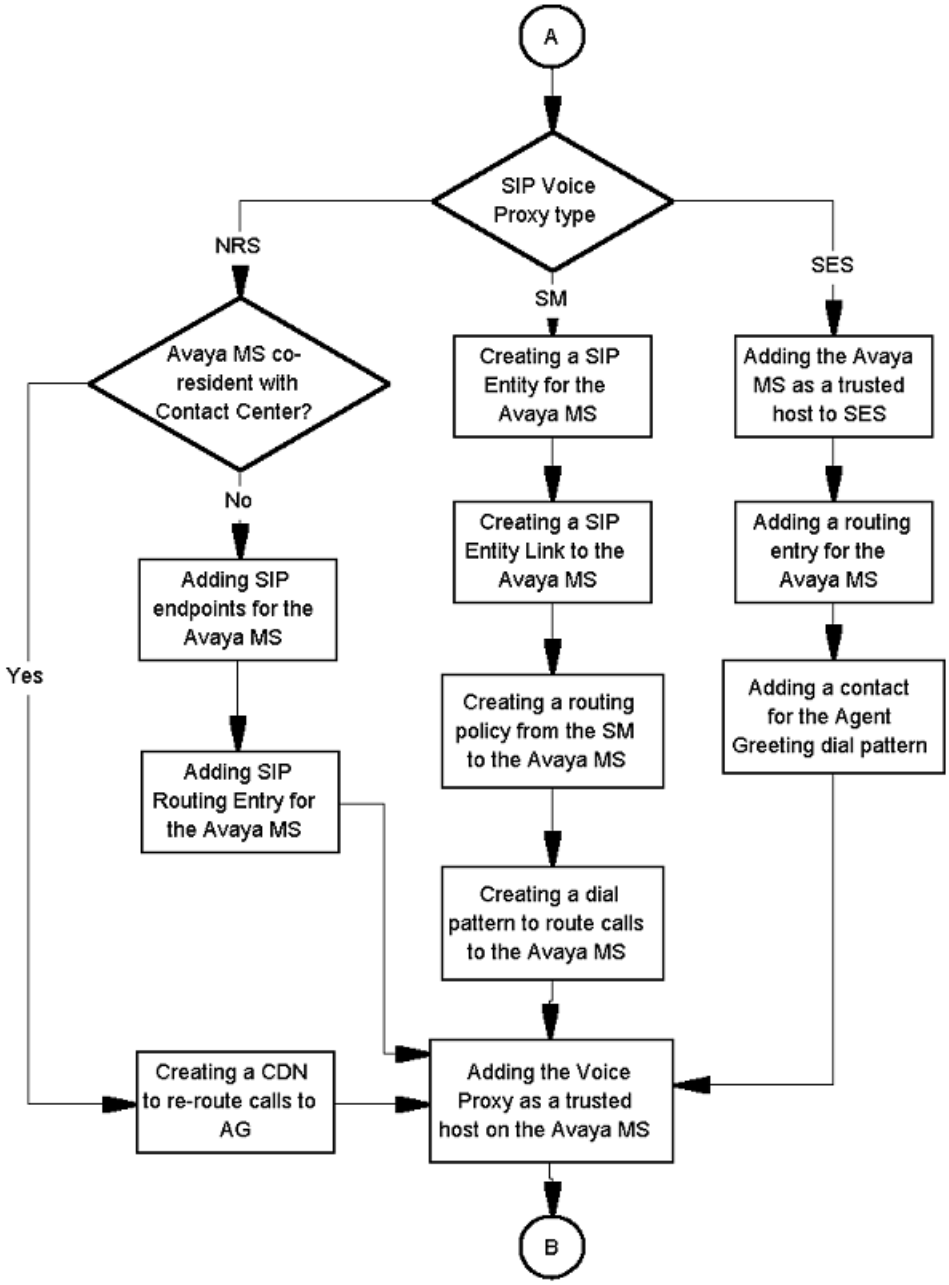


Figure 39: Agent Greeting commissioning navigation continued

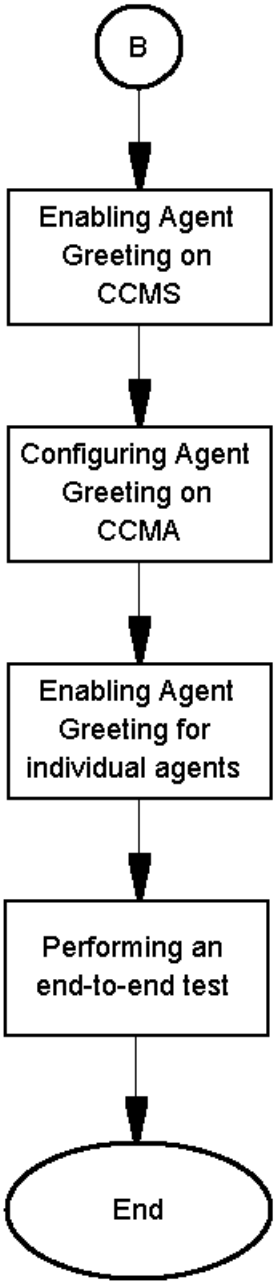


Figure 40: Agent Greeting commissioning navigation continued

Configuring Agent Greeting licensing on the Avaya Media Server

Before you begin

- You have ordered the software and received the keycode license sheet from Avaya.

Important:

You need to perform this procedure only if you have changed your Avaya MS license to support Agent Greeting after already commissioning your Avaya MS and contact center.

- You have administrator privileges on the Avaya Media Server Element Manager.

About this task

Follow this procedure to configure Agent Greeting licensing on the contact center Avaya Media Server. You apply an Avaya MS license file with the Agent Greeting feature to enable agents to record their greetings. If your contact center uses more than one Avaya MS, apply the license file to the primary license server.

Procedure

1. Access the Avaya Media Server Element Manager with Administrator privileges.
2. Expand **Licensing**.
3. Select **General Settings**.
4. On the General Settings screen, select **License Server**.
5. Copy the keycode and paste it into the **Add License Keys** field.
6. Click **Validate**.
7. Click **Save**.

Configuring Agent Greeting on the Avaya Media Server

About this task

Configure the Avaya Media Server to connect to the Contact Center Manager Server (CCMS) and the Contact Center Manager Administration (CCMA) servers in the contact center.

You can specify more than one CCMS server but only one CCMA server. The CCMA server you configure must manage all the CCMS servers.

Procedure

1. Access the Avaya Media Server Element Manager with Administrator privileges.
2. In the navigation pane, click **Applications** > **Packaged Applications** > **Contact Center** > **Agent Greeting**.
3. In the **Contact Center Connectivity** section, enter the IP address, Username, and Password for the CCMA server that manages the CCMS servers in your contact center.
4. Enter the IP address of each CCMS server in the contact center.
5. If you want to restrict the allowed number of incorrect Agent Greeting log on attempts, complete the boxes under **General Settings**.
6. Click **Save**.

Variable definitions

Name	Description
Contact Center Manager Administration (CCMA) IP Address	The IP Address of the CCMA server that manages the CCMS servers in your contact center.
CCMA Username	Enter the username of a CCMA user with full administration permissions. Agent Greeting uses this username to log on to the CCMA database.
CCMA Password	Enter the password for the CCMA user.
Contact Center Manager Server (CCMS) IP Address	The IP Address of a CCMS server where Agent Greeting is enabled.
Maximum Login Attempts	The maximum number of allowed incorrect log on attempts before Agent Greeting disables log on for the agent.
Account Disabled Period (seconds)	The amount of time in seconds that Agent Greeting keeps an agent's account disabled if they have exceeded the allowed number of incorrect log on attempts.

Configure a CDN to re-route calls to Agent Greeting

About this task

Use this procedure to configure a CDN that a co-resident contact center using a CS1000 NRS can use to re-route SIP calls to the Agent Greeting recording application.

Procedure

1. Create or select a route on the CS 1000 that directs agent calls to the Contact Center.
2. Create or select a CDN on CCMS that you can use to route calls to Agent Greeting through an Orchestration Designer application.
3. Log on to CCMA with administrative privileges.
4. Select **Scripting**.
5. Create an application in Orchestration Designer to route calls on this CDN to the URI of the Agent Greeting application on the co-resident Avaya Media Server. Enter the URI in the form `1234@AA.BB.CC.DD:5070`, where “1234” is the CDN and “AA.BB.CC.DD” is the IP address of the co-resident server.
6. Save and activate the Orchestration Designer application.
7. Note the CDN used and enter the same number in the **Agent greeting record number** when configuring the Agent Greeting settings in CCMA. For more information about the Agent Greeting settings, see Configuring Agent Greeting on CCMA on page 280.

Procedure job aid

Create an Orchestration Designer application to route calls from agents to the Agent Greeting application on the Avaya Media Server.

In this example the administrator has created a CDN “1234” on CCMS, and the co-resident Contact Center server IP address is “47.82.22.15”. The administrator creates an application in Orchestration Designer with a Logic block to check the CDN. If the CDN is “1234”, the flow passes to a Finish block “ROUTE TO AG”.

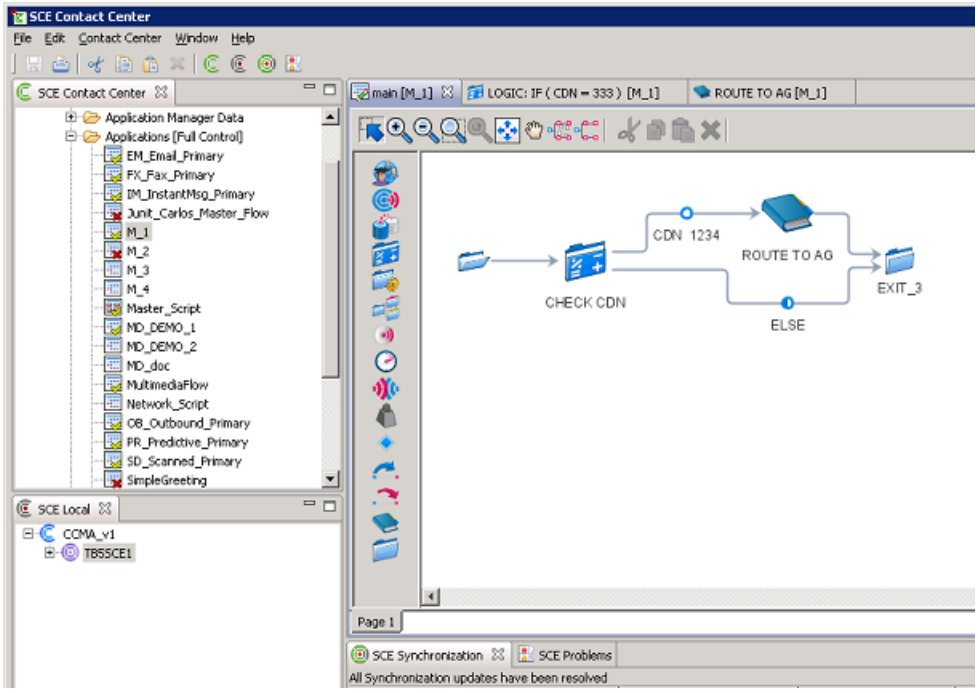


Figure 41: Example of a flow testing for the CDN

In the Finish block “ROUTE TO AG”, the administrator configures the URI of the Agent Greeting application on the co-resident Avaya Media Server, in the form `1234@47.82.22.15:5070`.

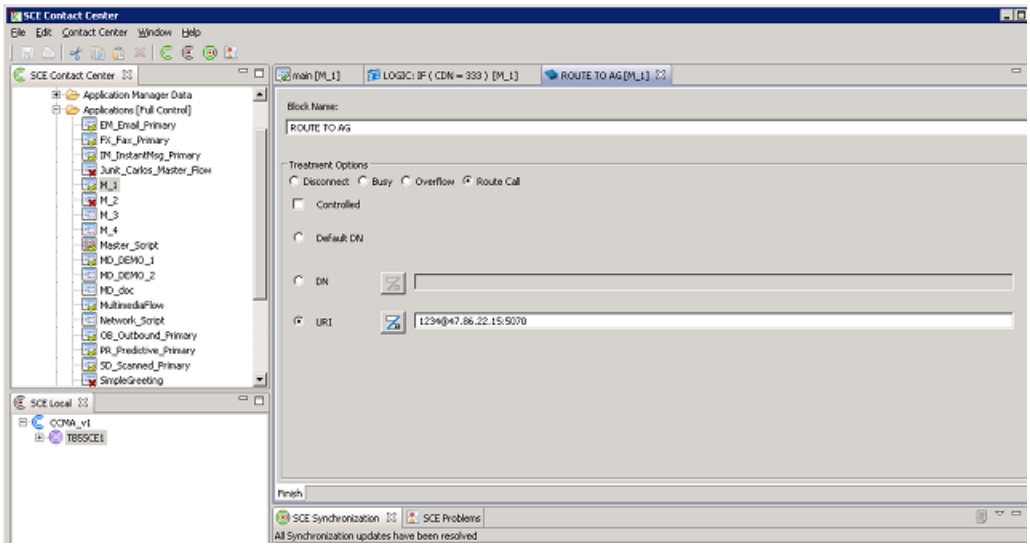


Figure 42: Example of an Agent Greeting application URI in a Finish block in Orchestration Designer

Adding SIP endpoints for the Avaya Media Server

About this task

Add the Avaya Media Server as a static endpoint to the Network Routing Service (NRS). This allows you to add routing entries.

Various types of Network Routing Services are available for the Avaya Communication Server 1000, such as SIP Redirect Server (SRS) or SIP Proxy Server (SPS).

Procedure

1. Log on to the NRS.
2. In the navigation pane, expand the **Numbering Plan** option.
3. Click **Endpoints** > **Gateway Endpoints**.
4. Under Managing, click **Standby database**.
5. In the **Limit results to Domain**, select the appropriate domain from the **All service domains** list.
6. In the **Limit results to Domain**, select the appropriate domain from the **All L1 domains** list.
7. In the **Limit results to Domain**, select the appropriate domain from the **All L0 domains** drop-down list. The new Endpoint is added to this domain and the Add button is enabled.
8. Click **Add**.
9. In the **End point name** box, type the name of the Avaya Media Server.
10. In the **Description** box, type a descriptive name for the Avaya Media Server.
11. In the **Endpoint authentication enabled** list, select **Authentication off**.
12. Scroll down to find the Static endpoint address field.
13. In the **Static endpoint address** box, type the IP address of the Avaya Media Server.
14. From the **SIP support** list, select **Static SIP endpoint**.
15. Select **TCP transport enabled**. (UDP may also be selected, TLS is not yet supported).
16. Click **Save**.
17. In the left pane, click **System** > **Database**.
18. Click **Cut over**.

19. Click **Commit**.

Adding SIP Routing Entry for the Avaya Media Server

Before you begin

- Know the dialing plan entry.

About this task

This procedure outlines how to add a SIP Routing Entry for the Avaya Media Server on the NRS.

Routing entries ensure the NRS can decide when to forward calls to the Avaya Media Server endpoint.

Procedure

1. Log on to the NRS.
2. In the navigation pane, expand the **Numbering Plan** option.
3. Click **Routes** > **Gateway Endpoint**.
4. Under **Managing** click on the **Standby database**.
5. In the **Limit results to Domain**, select the appropriate domain from the **All service domains** list.
6. In the **Limit results to Domain**, select the appropriate domain from the **All L1 domains** list.
7. In the **Limit results to Domain**, select the appropriate domain from the **All L0 domains** list.
8. Click **Add**.
9. In the **DN type** list, select the appropriate Dial Plan.
10. In the **DN prefix** box, type the number that agents dial to log on to the Agent Greeting application.
11. Enter a **Route cost** to support least-cost routing, usually 1.
12. Click **Save**.
13. In the left pane, click **System** > **Database**.
14. Click **Cut over**.

15. Click **Commit**.

Creating a SIP Entity for Avaya Media Server

Before you begin

- Ensure you create a routing domain and a routing location.

Important:

The port parameter is mandatory when CCMS and Avaya Media Server are co-resident. The Avaya Media Server uses port 5070 when it is co-resident with other Contact Center components.

About this task

Create a SIP Entity for the Avaya Media Server. To administer minimal routing to Avaya Media Server, you must configure a SIP entity of type Session Manager and configure the Avaya Media Server as type Other.

If your Avaya Media Server supports High Availability (HA) then the IP address for the Avaya Media Server SIP Entity is the Avaya Media Server HA pair cluster IP address.

If you have more than one Avaya Media Server but do not use High Availability (HA) then the IP address for the Avaya Media Server SIP Entity is the Avaya Media Server cluster master server IP Address.

Procedure

1. On the System Manager console, select **Routing** > **SIP Entities**.
2. Click **New**.
3. In the **Name** box, type the name of the Avaya Media Server SIP Entity. Avaya recommends that you type a descriptive name for your Avaya Media Server SIP entity.
4. In the **FQDN or IP address** box, type the IP address of the Avaya Media Server or the managed IP address of the Avaya Media Server HA pair.
5. From the **Type** list, select **Other**.
6. In the **Location** box, select the location for this Avaya Media Server.
7. Enter a regular expression string in the Credential name field. The SM uses the Credential name for TLS connection validation by searching for this string in the SIP entity identity certificate.

8. Under SIP Link Monitoring, use the drop-down menu to select one of the following:
   —Use Session Manager Configuration - Use the settings under **Session Manager – Session Manager Administration**.
   —Link Monitoring Enabled - Enables link monitoring on this SIP entity.
   —Link Monitoring Disabled - Disables link monitoring on this SIP entity.
9. If CCMS and the Avaya Media Server are co-resident, click **Add** under **Port** and specify the Port and Protocol parameters.
   When Session Manager receives a request where the host-part of the request-URI is the IP address of the Session Manager, it associates one of the administered domains with the port on which the request was received.
10. Click **Commit**.

Variable definitions

Name	Description
Name	SIP entity name. This name must be unique and can have between 3 and 64 characters.
FQDN or IP Address	Fully qualified domain name or IP address of the Avaya Media Server SIP entity. If your Avaya Media Server supports High Availability (HA) then the IP address for the Avaya Media Server SIP Entity is the Avaya Media Server HA cluster IP address. If your Avaya Media Server does not support High Availability (HA) then the IP address for the Avaya Media Server SIP Entity is the Avaya Media Server IP Address.
Type	SIP entity type, such as Other.
Notes	Additional notes about the SIP entity.
Adaptation	Adaptation to be used for the SIP entity. Select from already defined adaptations.
Location	SIP entity location. Select from previously defined locations.
Outbound Proxy	Outbound proxy if the entity type is Session Manager, and you wish to specify a proxy.
Time Zone	Time zone for the SIP entity.

Name	Description
Override Port & Transport with DNS SRV	Specify if you wish to use DNS routing. SIP uses DNS procedures to allow a client to resolve a SIP URI into the IP address, port, and transport protocol of the next hop to contact. It also uses DNS routing to allow a server to send a response to a backup client if the primary client fails.
SIP Timer B/F (Seconds)	Amount of time the Session Manager waits for a response from the SIP entity.
Credential name	Enter a regular expression string in the Credential name. Credential name is used for TLS connection validation by searching this string in the SIP entity identity certificate.
Call Detail Recording	Select or clear the check box to turn SIP monitoring on or off.
Proactive cycle time (Seconds)	Enter a value between 120 and 9000 seconds. The default is 900. This specifies how often the entity is monitored when the link to the entity is up or active.
Reactive cycle time (Seconds)	Enter a value between 30 and 900 seconds. The default is 120. This specifies how often the entity is monitored when a link to the entity is down or inactive.
Number of retries	Enter a value between 0 and 15. The default is 1. This specifies the number of times Session Manager tries to ping or reach the SIP entity before marking it as down or unavailable.
Port	Add a listening port for the SIP entity.
Protocol	The protocol that the SIP entity uses.
SIP Domain	The domain of the SIP entity.
Notes	Additional notes about the port and port parameters.

Creating a SIP Entity Link to the Avaya Media Server

Before you begin

- Ensure you have created a SIP Entity for the Avaya Media Server.

About this task

Session Manager enables you to create an entity link between the Session Manager and any other administered SIP entity.

Create a SIP entity link from the Session Manager to the Avaya Media Server. You must configure an entity link between a Session Manager and any entity that you have administered, if you want the Session Manager to be able to send messages to, or receive messages from, that entity directly. To communicate with other SIP entities, each Session Manager instance must know the port and the transport protocol of its entity link to these SIP entities in the network.

For Agent Greeting, create a SIP entity link from the Session Manager to the Avaya Media Server.

Procedure

1. On the System Manager console, select **Routing** > **Entity Links**.
2. Click **New**.
3. In the **Name** box, type the name for this SIP Entity Link. Avaya recommends that you type a descriptive name for your SIP Entity Link.
4. Under **SIP Entity 1**, select the required Session Manager SIP entity from the drop-down list and provide the required port number.

   SIP entity 1 must always be a Session Manager instance.

   The default port for TCP is 5060.

   If the Avaya MS is co-resident with other Contact Center components, you must set this port to 5070.
5. From the Protocol list, select **TCP**.
6. Under **SIP Entity 2**, select the required Avaya Media Server SIP entity from the drop-down list and provide the required port number.

   The port number is the port on which you have configured Avaya Media Server to receive requests for the specified transport protocol.

   The default port for TCP is 5060.

   If the Avaya MS is co-resident with other Contact Center components, you must set this port to 5070.

7. If the Avaya Media Server SIP entity is trusted, select the **Trusted** check box. Session Manager does not accept SIP connection requests or SIP packets from untrusted SIP entities.
8. Click **Commit**.

Creating a routing policy from Session Manager to the Avaya Media Server

About this task

Create a routing policy from Session Manager to Avaya Media Server.

Routing policies can include the “Origination of the caller”, the “dialed digits” of the called party, the “domain” of the called party, and the actual time the call occurs. Optionally, instead of “dialed digits”, and the “domain” of the called party, the administrator can define a “regular expression” to create a routing policy.

For Agent Greeting, create a routing policy from Session Manager to Avaya Media Server.

Depending on one or multiple inputs mentioned above a destination where the call must be routed is determined. Optionally, the destination can be qualified by “deny” which means that the call is not routed.

Session Manager uses the data configured in the Routing Policy to find the best match against the number (or address) of the called party.

Procedure

1. On the System Manager console, select **Routing** > **Routing Policies**.
2. Click **New**.
   The Routing Policy Details screen appears.
3. In the **General** section, in the Name box, type the name for the Routing Policy. Avaya recommends that you type a descriptive name for your Routing Policy.
4. In the **Notes** box, type your notes about this Routing Policy.
5. In the **SIP Entities as Destination** section, click **Select**.
6. From the list of SIP Entities, select the SIP Entity for your Avaya Media Server.
7. Click Select.
8. If you need to associate the Time of Day routing parameters with this Routing Policy, click **Add** from the **Time of Day** section.

9. Select the Time of Day patterns that you want to associate with this routing pattern.
10. Click **Select**.
11. Click **Commit**.

Creating a dial pattern to route calls to the Avaya Media Server

About this task

Create a dial pattern using the Avaya Media Server Session Manager to Avaya Media Server Routing Policy. Session Manager uses this dial pattern to route calls to the Avaya Media Server for Agent Greeting.

A dial pattern specifies which routing policy or routing policies are used to route a call based on the digits dialed by a user which match that pattern. The originating location of the call and the domain in the request-URI also determine how the call gets routed.

For Agent Greeting, create a dial pattern using the Session Manager to Avaya Media Server Routing Policy.

Session Manager tries to match the Request-URI of a request to a row in the dial pattern table. The rows considered for the match are all rows where:

- The domain in the dial pattern table matches the domain in the request-URI
- The originating location in the dial pattern table row matches the originating location of the request, or, if there are no rows matching the originating location, the originating location in the table is set to -ALL-, or, if there was no originating location, the originating location in the table is -ALL-
- The digit pattern in the row matches the user-part of the request-URI, ignoring any parameters that are in the user part of the request-URI

Procedure

1. On the System Manager console, select **Routing** > **Dial Patterns**.
2. Click **New**.
   The Dial Pattern Details screen appears.
3. In the **General** section, type the Dial Pattern General information. Note that a **Domain** can be provided to restrict the Dial Pattern to the specified Domain.
4. Under the **Originating Locations and Routing Policies** section, click **Add**.

5. Select all the required Locations and Routing Policies that you want associated with the Dial Pattern by selecting the check box in front of each item.
6. From **Routing Policy Name**, select the Session Manager to Avaya Media Server Routing Policy.
7. From the **Routing Policy Destination**, select the Avaya Media Server SIP Entity.
8. Click **Select** to indicate that you have completed your selections.
9. If you need to specify the calls from the specified locations are denied, click **Add** under the **Denied Originating Locations** section.
10. Select all the Locations that are to be denied and click **Select** to indicate that you have completed your selections.
11. Click **Commit**.

Adding the Avaya Media Server as a trusted host on the SES

About this task

Add the Avaya Media Server to the list of trusted hosts on the SIP Enablement Services (SES) server.

Procedure

1. In the left pane of the SIP Server Management Integrated Management console, click **Trusted Hosts**.
2. Click **Add Trusted Hosts**.
   The Add Trusted Host page appears.
3. In the **IP Address** box, type the IP address of the Avaya Media Server.
4. From the **Host** list, select the server to accept the SIP request from the Agent Greeting server you specified.
5. Click **Add**.
6. Click **Continue**.

Adding a routing entry for the Avaya Media Server

About this task

Add the Avaya Media Server routing entry to the SIP Enablement Services (SES) server. This indicates to the SES which host (SIP endpoint) to send calls to, based on the dialed number.

Procedure

1. In the left pane of the SIP Server Management Integrated Management console, click **Hosts**.
2. Click **List Hosts**.
   The list of hosts appears.
3. From the **List Hosts**, identify the host to modify. The host in this case is the SES server. Click **Map** for the SES server IP address.
4. Click **Add Map In New Group**.
   A new Add Host Address Map page appears.
5. In the **Name** box, type the name of the map entry.
6. In the **Pattern** box, type the number that the agents dial to log on to the Agent Greeting application.
7. Clear **Replace URI**. This replaces the Communication Manager SIP domain with the SES IP address in the outgoing messages to Avaya Media Server.
8. Click **Add**.
9. Click **Continue**.

Adding a contact for the Agent Greeting dial pattern

Before you begin

- Ensure that there is an Avaya Media Server routing entry to the SES server.

About this task

Add contact details for the Avaya Media Server routing entry. This configures the SES server to send calls to the Contact Center Manager Server when the calls match the map.

Procedure

1. In the SIP Server Management Integrated Management console, under Host Lists, select the Avaya Media Server address map.
2. Click **Map**.
3. Click **Add Another Contact**.
   The Add Host Contact page appears.
4. In the **Contact box**, type the number that the agents call to access the Agent Greeting recording application.
5. Click **Add**.

Adding the Voice Proxy server as a trusted host on the Avaya MS

About this task

Use this procedure to add the SIP Voice Proxy server (SM, NRS, or SES) to the list of trusted hosts on the Avaya MS.

Procedure

1. Access the Avaya Media Server Element Manager with Administrator privileges.
2. In the navigation pane, click **System Configuration** > **Signalling Protocols** > **SIP** > **Nodes and Routes**.
3. Click **Trusted Nodes**.
4. Click **Add**.
   Avaya MS displays the Add SIP Trusted Node screen
5. Type the IP address of the Voice Proxy server (the SM, NRS, or SES) in the **Host or Server Address**.
6. Click **Save**.

Enabling Agent Greeting on CCMS

Before you begin

Important:

You need to restart the CCMS server to complete this procedure.

About this task

Follow this procedure to enable Agent Greeting on CCMS.

Procedure

1. Log on to the server on which you installed Contact Center Manager Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
3. Click the **Licensing** tab.
4. From the **CCMS Optional Packages** list, select **Agent Greeting**.
5. Click **OK**.
6. Click **Yes** to restart the server.

Configuring Agent Greeting on CCMA

Before you begin

Important:

If you restarted your CCMS server after applying the Agent Greeting license, refresh the CCMS server in CCMA to be able to see the Agent Greeting configuration fields.

Important:

Changes to these settings can take up to ten minutes to take effect.

About this task

Follow this procedure to set the general system settings for Agent Greeting on CCMA. These system wide settings control the operation of the Agent Greeting feature. The playback configuration settings apply to all Agent Greeting playbacks.

Modifying these settings on an existing Agent Greeting solution does not affect greetings already in progress.

Procedure

1. Log on to Contact Center Manager Administration with administrator privileges.
2. On the **Launchpad**, click **Configuration**.
3. In the system tree, expand the server on which to configure Agent Greeting.
4. In the left pane, click **Agent Greeting**.
5. Under **General Settings**, select the options that you want to enable.
6. Under **Time of Day Settings**, select the options that you want to enable.
7. Click **Save**.

Variable definitions

Name	Description
Agent Greeting enabled	Select to enable Agent Greeting.
Mute agent on greeting playback	Select to automatically mute the agent while the greeting plays.
No greeting warning tone	Select to ensure that the caller hears a beep if agent has not recorded a greeting.
Allow an agent to interrupt the greeting	Select to allow an agent to terminate the greeting to speak directly to the caller.
Maximum allowed greeting length	The maximum length of the greeting that the agent is allowed to record. Valid values: 1 to 30 seconds. This setting can take up to ten minutes to take effect. Reducing the maximum allowed greeting length does not affect greetings that are already recorded, even if they are longer than the new allowed maximum.
Agent greeting record number	This is the number on the PABX that routes to the Agent Greeting application on the Avaya Media Server. This setting can take up to ten minutes take effect.

Name	Description
Prompt language	Lists the languages from which you can choose a language for the application prompts. Agents hear the selected language when they dial into the recording application. This setting can take up to ten minutes take effect.
Enable time of day greetings	Select to enable or disable the playback of time of day greetings.
Morning start time	Select to specify the time after which the system plays morning greetings.
Afternoon start time	Select to specify the time after which the system plays afternoon greetings.
Evening start time	Select to specify the time after which the system plays evening greetings.
Playback position	Select to specify whether the time of the day greeting plays before or after the main greeting.

Enabling Agent Greeting in a voice-only Agent Desktop contact center

About this task

In a voice-only Agent Desktop contact center, you must configure Agent Greeting settings using a configuration tool. You configure Agent Greeting to be enabled or disabled.

Note:

If you enable Agent Greeting, the Agent Greeting button appears on the Agent Desktop for all agents. If an agent who you have not configured for Agent Greeting clicks the Agent Greeting button, they hear a voice prompt to log on but cannot access the Agent Greeting application.

Procedure

1. Log on to the active Communication Control Toolkit server.
2. Navigate to `<Installed Drive>:\Avaya\Contact Center\Multimedia Server\Agent Desktop\.`
3. Double-click `CCADConfigurator.exe` to start the Agent Desktop Toolbar configuration utility.

4. On the password message box, type the password. The default password is "__avaya".
5. Click **OK**.
6. On the **App Settings** tab, in the **AGEnabled** row, in the **Value** column type `true`.
7. In the **AGNumber** row, in the **Value** column type the Agent Greeting record number. This is the number on the PABX that routes to the Agent Greeting application on the Avaya Media Server.

Enabling Agent Greeting for individual agents

About this task

You must enable Agent Greeting for each individual agent. By default, Agent Greeting is disabled for each agent. Therefore, even if Agent Greeting is globally enabled, Agent Greeting does not play until it is enabled for the individual agents.

Procedure

1. Log on to Contact Center Manager Administration with administrative privileges.
2. On the Launchpad, click **Contact Center Management**.
3. In the left pane, expand the Contact Center Manager Server on which you want to modify the agent.
4. Select the agent and scroll to the **Agent Greeting** tab. Select the **Agent Greeting Enabled** check box.
5. Type a numeric password in the **Agent Greeting Password** box. This is the password the agent uses to log on to the Agent Greeting recording application.
6. Click **Submit**.

Performing an end-to-end test

Before you begin

- Ensure you complete all relevant installation and commissioning procedures in both *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611) and this guide.
- Ensure your contact center is operational.

About this task

After completing all the commissioning steps in this chapter, configure an agent for Agent Greeting and test that the agent can log in to Agent Greeting and record their greetings. Place a test call to the contact center to ensure the greeting plays as intended.

Procedure

1. Enable Agent Greeting on the CCMS server.
2. Enable Agent Greeting for an agent.
3. Use the agent details to log on to the contact center.
4. Dial the number you configured for the Agent Greeting application.
5. Verify that you can access the Agent Greeting recording application.
6. Configure the default greeting for the agent, and optionally one or more skillset greetings.
7. Place a call to the contact center for this agent's skillset.
8. Verify that the agent's greeting plays when the agent answers the call.

Chapter 20: Office Communications Server commissioning

This section describes how to configure the Microsoft Office Communications Server (OCS) 2007. Use the OCS as a platform to configure the Instant messaging tool in a SIP-enabled Contact Center environment.

For OCS environments with multiple OCS Enterprise Edition pools or Standard Edition Front End (FE) servers, you must configure these settings for each pool or FE server. A static route configured on one pool or one FE server is not visible to other pools or FE servers in the domain.

For federated users to access the SIP-enabled contact center where OCS edge servers and OCS directors are employed, apply this configuration to the OCS directors as well.

For nonfederated instant messaging, the static route matching URI can be any string. For federated IM, the wildcard must be the same as the service domain or the domain that is federated with third-party organizations.

Office Communications Server commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to configure the Office Communications Server.

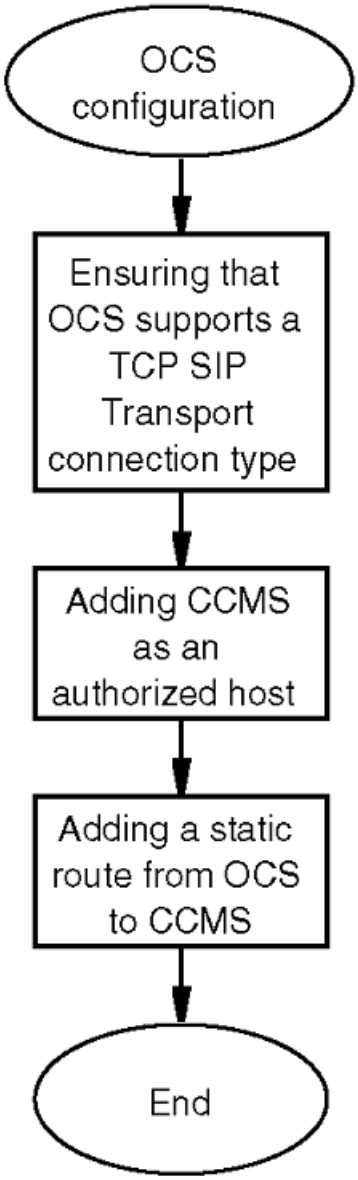


Figure 43: Office Communications Server configuration procedures

Ensuring that OCS supports TCP SIP Transport connection type

About this task

Ensure that OCS supports TCP SIP Transport connection type to enable OCS to communicate with SIP-enabled contact center.

Procedure

1. Open the Microsoft Office Communications Server 2007 console snap-in.
2. Expand the tree.
3. Click the SIP Contact Center OCS server.
4. In the **Front End Server** section, ensure that **5060** appears under **Port** and the **TCP** appears under **Transport**.

Procedure job aid

The following figure shows an Office Communications Server configured for TCP SIP Transport type.

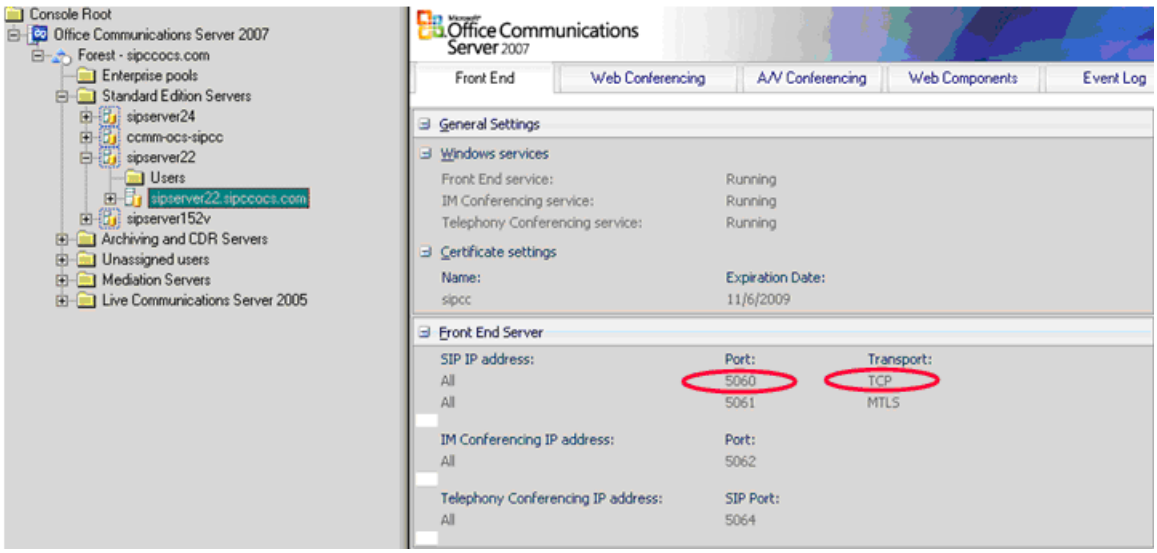


Figure 44: OCS 2007

Adding Contact Center Manager Server as an authorized host

About this task

Add the Contact Center Manager Server as an authorized host on the Office Communications Server to enable communication between the two.

Procedure

1. Open the Microsoft Office Communications Server 2007 console snap-in.
2. Expand the tree.
3. Click the **Front Ends** folder.
4. Right-click the OCS server, and then select **Properties**.
5. On the **Front End Properties** dialog box, click the **Host Authorization** tab.
6. Click **Add**.
7. On the **Add Authorized Host** dialog box, select **IP address** and type the IP address of the Contact Center Manager Server.
8. Under **Settings**, select **Throttle As Server** and **Treat As Authenticated**.
9. Click **OK**.
10. On the **Front End Properties** dialog box, click **OK**.

Adding a static route from OCS to Contact Center Manager Server

About this task

Add a static route from OCS to Contact Center Manager Server to enable communication between the two servers.

When you add Contact Center Manager Server as a trusted node in an OCS pool, add each Front End server to the trusted list as well. This is required for instant messages that originate from Contact Center Manager Server to be routable by the Front End servers internal to the pool.

Procedure

1. Open the Microsoft Office Communications Server 2007 console snap-in.
2. Expand the tree.
3. Click the **Front Ends** folder.
4. Right-click the OCS server, and then select **Properties**.
5. On the **Front Ends Properties** dialog box, click the **Routing** tab.
6. Click **Add**.
7. On the **Add Static Route** dialog box, under **Matching URI**, in the **Domain** box, type the name for the domain.

   For nonfederated instant messaging, the static route matching URI can be any string. For federated IM, the wildcard can be the same only as the service domain or the domain that is federated with third-party organizations.
8. Under **Next Hop**, select **IP address** and type the IP address of the Contact Center Manager Server.
9. From the **Transport** list, select **TCP**.
10. In the **Port** box, type the port number.
11. Click **OK**.
12. On the **Front Ends Properties** dialog box, click **OK**.

Chapter 21: Avaya Aura® Presence Services Instant Messaging application commissioning

Commission the Instant Messaging application to allow customers to start Instant Messaging chat sessions with the contact center.

This chapter contains procedures to commission the Avaya sample chat server application that you install on your external Web server. For custom integrations substitute your customer application in place of the Avaya sample application.

Presence Services Instant Messaging chat server commissioning prerequisites

About this task

- The contact center is SIP-enabled and uses the Avaya Aura® Release 6.1 or 6.2 communication platform.
- You have installed and commissioned the System Manager server and the Presence Services server.
- You are familiar with System Manager user administration and maintenance. See documentation on administering Avaya Aura® System Manager.
- You have installed the sample Instant Messaging chat server on the external web server. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- You have created a customer user account on the Presence Services server. See documentation on administering Avaya Aura® Presence Services.

Presence Services Instant Messaging chat server commissioning procedures

About this task

This task flow shows you the sequence of procedures you perform to commission the sample Presence Services Instant Messaging chat server. For a custom integration most of these procedures also apply.

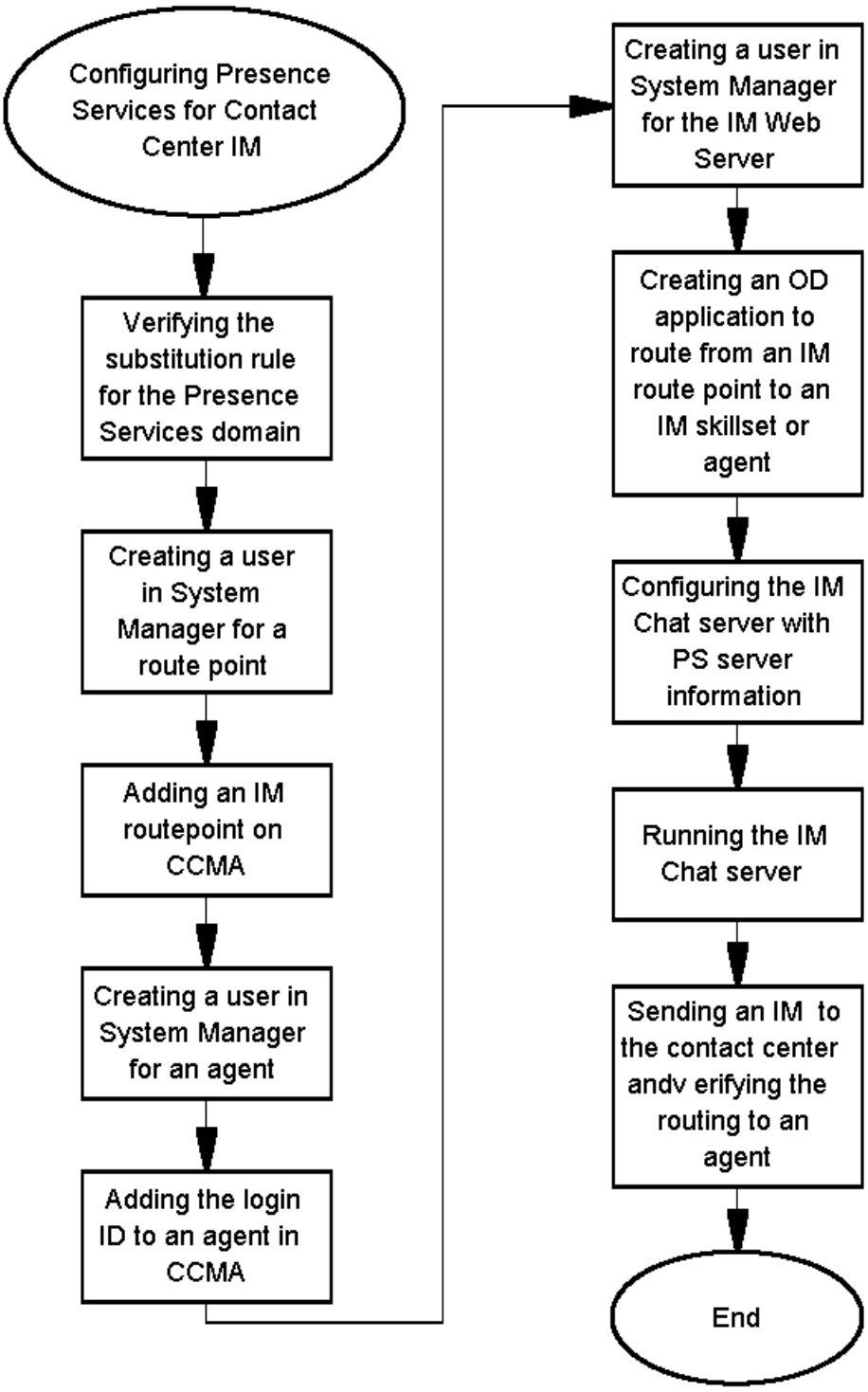


Figure 45: Instant Messaging chat server commissioning procedures

Verifying the substitution rule to map the System Manager user login domain to the Presence Services domain

About this task

Use this procedure to verify the substitution rule that maps the System Manager user login domain to the Presence Services domain.

The domain substitution rule ensures that System Manager provisions a matching account on the Presence Services server for each user created. When this rule is in place, if you add a SIP handle to a user's communication profile System Manager automatically provisions an XMPP handle in Presence Services.

The XMPP handle is what Presence Services uses to communicated with the IM Route Points, agent URIs, and the IM chat server address.

Normally the substitution rule exists on a fully commissioned Presence Services server.

Procedure

1. Log on to the System Manager console.
2. Under **Elements**, select **Presence** > **Configuration**.
3. If the substitution rule is not correct for your implementation, complete steps 4 to 7.
4. Click **Edit**.
5. In the **Domain Substitution - From** field type the domain you are mapping from (System Manager user domain).
6. In the **Domain Substitution - To** field type the Presence Services XMPP domain.
7. Click **Save**.

Variable definitions

Name	Description
Domain Substitution - From	The domain you are mapping from (System Manager user domain).
Domain Substitution - To	The Presence Services XMPP domain.

Creating a Presence Services user in System Manager for the route point

About this task

Use this procedure to create a user in System Manager which the Presence Services server uses to route instant messages to the contact center.

Procedure

1. Log on to the System Manager console.
2. Under **Users**, select **Manage users**.
3. Click **New**.
4. On the **Identity** tab, complete the user details.
5. Select the **Communications Profile** tab.
6. Under **Communications Address**, click **New**.
7. Complete the **Shared Communication Profile Password**, **Type** and **Fully Qualified Address** fields.
8. Click **Add**.
9. Click **Commit**.

Variable definitions

Name	Description
Last Name	Avaya recommends that you enter a descriptive name that identifies the user as being for a route point. For example, “routepoint”.
First Name	Avaya recommends that you enter a descriptive name that identifies the user as being for a route point. For example, use the route point number.
Description	Avaya recommends that you enter a description that identifies the user as being

Name	Description
	for a route point, and how the contact center uses the route point.
Login Name	Enter a login name for the route point user in the following format: <username>@<domain>.<com> The domain specified must have a substitution rule in System Manager mapping it to the Presence Services domain.
Authentication Type	The authentication type defines how the system performs this user's authentication. Select **Basic**.
Password	Enter a password for the user.
Confirm Password	Confirm the password for the user.
Shared Communication Profile Password	For a Route Point the password must be a hyphen "-".
Type	Select Avaya SIP.
Fully Qualified Address	The SIP domain handle for this user account (entering this automatically provisions an XMPP handle for the Presence Services server.)

Adding an IM route point on CCMA for Presence Services

Before you begin

- Log on to CCMA and open the Configuration component.

About this task

Use this procedure to add an Instant Message route point on CCMA.

Procedure

1. In the left pane, expand the SIP-enabled **Contact Center Manager Server** to which to add the CDN (Route Point).
2. Select the **CDNs (Route Points)** folder.
3. In the right pane, in the **Name** box, type the name of the CDN (Route Point) as you want it to appear in reports.
4. In the **Number** box, type the CDN (Route Point) number.

5. In the **URI** box, type the XMPP handle for the user you created for this route point on the System Manager.
6. From the **Call Type** list, select **Local**.
7. Click any other row of the table to add the CDN (Route Point).
   Not Acquired appears in the **Status** column.
8. Select the **Acquired?** check box for the CDN (Route Point) Landing Pad.
9. Click any other row of the table to acquire the CDN (Route Point) Landing Pad.
10. Click **Refresh Status** to view the current status.

Creating a Presence Services user in System Manager for an agent

About this task

Use this procedure to create a user in System Manager for a contact center agent. Each agent that handles IM contacts must have a Presence Services user.

Procedure

1. Log on to the System Manager console.
2. Under **Users**, select **Manage users**.
3. Click **New**.
4. On the **Identity** tab, complete the user details.
5. Select the **Communications Profile** tab.
6. Under **Communications Address**, click **New**.
7. Complete the **Shared Communication Profile Password**, **Type** and **Fully Qualified Address** fields.
8. Click **Add**.
9. Click **Commit**.

Variable definitions

Name	Description
Last Name	Enter the agent's last name.
First Name	Enter the agent's first name.
Login Name	Enter a login name for the agent in the following format: <username>@<domain>.<com> The domain specified must have a substitution rule in System Manager mapping it to the Presence Services domain.
User Type	Select **Agent**.
Authentication Type	The authentication type defines how the system performs this user's authentication. Select **Basic**.
Login Password	Enter a password for the agent.
Confirm Password	Confirm the password for the agent.
Shared Communication Profile Password	Enter the password for this agent to use to log on in the Presence Services tab on Agent Desktop.
Type	Select Avaya SIP.
Fully Qualified Address	The SIP domain handle for this user account (entering this automatically provisions an XMPP handle for the Presence Services server.)

Adding the login ID to an agent's settings in CCMA

Before you begin

- Log on to CCMA and open the Contact Center Management component.
- Ensure that you have access to the agent record that you want to change.

About this task

Use this procedure to link an agent's Presence Services user account to their contact center configuration.

Comments? infodev@avaya.com

Procedure

1. From the **View/Edit** menu, select **Supervisors**.
2. In the left pane, click the server on which to work with the supervisor/agent profile.
   The list of supervisors configured on the server appears.
3. Click the supervisor to whom the agent is assigned.
   The tree expands to show the list of agents assigned to this supervisor.
4. Right-click the agent whose profile you want to edit, and then select **View Agent Details**.
   The Supervisor/Agent Details window appears.
5. In the **IM URI** menu, enter the XMPP handle of the user you created on System Manager for this agent.

Creating a Presence Services user in System Manager for the IM web server

About this task

Use this procedure to create a user in System Manager which the Presence Services server uses to exchange messages with the IM web interface.

Procedure

1. Log on to the System Manager console.
2. Under **Users**, select **Manage users**.
3. Click **New**.
4. On the **Identity** tab, complete the user details.
5. Select the **Communications Profile** tab.
6. Under **Communications Address**, click **New**.
7. Complete the **Shared Communication Profile Password**, **Type** and **Fully Qualified Address** fields.
8. Click **Add**.
9. Click **Commit**.

Variable definitions

Name	Description
Last Name	Avaya recommends that you enter a descriptive name that identifies the user as being for the IM Web server.
First Name	Avaya recommends that you enter a descriptive name that identifies the user as being for the IM Web server.
Description	Avaya recommends that you enter a description that identifies the user as being for the IM Web server.
Login Name	Enter a login name for the Web server user in the following format: <username>@<domain>.<com> The domain specified must have a substitution rule in System Manager mapping it to the Presence Services domain.
User Type	Select Agent.
Authentication Type	The authentication type defines how the system performs this user's authentication. Select Basic.
Login Password	Enter a password for the user.
Confirm Password	Confirm the password for the user.
Shared Communication Profile Password	Enter the password for the sample Web chat application user. If you create your own application, you need to use this password in that application.
Type	Select Avaya SIP.
Fully Qualified Address	The SIP domain handle for this user account (entering this automatically provisions an XMPP handle for the Presence Services server.)

Creating an Orchestration Designer application to route from an IM route point to an IM skillset

Before you begin

- You are familiar with creating and editing flows in Orchestration Designer. See *Avaya Aura® Contact Center Configuration – Orchestration Designer Application Development* (NN44400-510).
- You have access to an Orchestration Designer client and privileges to create flows for this contact center.

About this task

Create an application in Orchestration Designer to route IM contacts from the IM route point to an IM skillset.

Procedure

1. In Orchestration Designer, create a new flow to route IM contacts.
2. Edit the flow elements to route IM contacts received on the IM route point to an IM skillset.

Configuring the Instant Messaging chat server with the Presence Services server details

About this task

Follow this procedure to modify the xmppchat.config file on the external Web server with the Presence Services server details. This enables the external Web server to start Instant Messaging chat sessions with the contact center.

Procedure

1. On the external Web server, browse to **<PATH>\etc**, where <PATH> is the location where you installed the sample application.
2. Right-click the **xmppchat.config** file, click **Open**, and select **Notepad**.
   The xmppchat.config file opens in Notepad.
3. Enter the Presence Services server parameters as shown in the following example:

```
<?xml version=“1.0” encoding=“UTF-8”?>
```

```
<xmppserver>
<xmppserverdomain> PS_domain </xmppserverdomain>
<xmppserveripaddress> IP_Address </xmppserveripaddress>
<xmppserverport> Port_number </xmppserverport>
<xmppserverusername> Username </xmppserverusername>
<xmppserverpassword> Password </xmppserverpassword>
<imroutepointlist>
<imroutepoint>Routepoint_1</imroutepoint>
<imroutepoint>Routepoint_2</imroutepoint> </imroutepointlist>
</xmppserver>
```

4. Save the file.

Variable definitions

Name	Description
PS_domain	The domain name of the Presence Services server. For example, pres.company.com.
IP_Address	The IP address of the Presence Services server.
Port_number	The port number of the Presence Services server, normally 5222.
Username	The username of the sample Web chat application user you created on the System Manager for the Web server.
Password	The password of the sample Web chat application user you created on the System Manager for the Web server.
Routepoint_1	The Instant Messaging route point XMPP address configured in CCMA and the Avaya Aura® System Manager. You must configure at least one IM routepoint.

Running the Instant Messaging chat server

About this task

Use the following procedure to run the Instant Messaging chat server on the external Web server.

Procedure

1. On the command prompt of the external Web server, browse to the directory where you installed the Instant Messaging chat server.
2. Run the following command to start the Instant Messaging chat server: `java -jar start.jar`

Sending an Instant Message to the contact center and verifying the routing to an agent

Before you begin

- Complete all configuration procedures in this chapter.
- Create an agent enabled for Presence Services and for the IM contact type, and assign the agent to an IM skillset.

About this task

Test the Instant Message chat server functionality by sending an Instant Message into the contact center and verifying that it routes to an agent to whom you can chat.

Procedure

1. On a client PC, open the Agent Desktop application and log in as an agent enabled for IM contact types and assigned to the skillset that you want to test.
2. Make the agent Ready on Agent Desktop.
3. On another client PC, start a Web browser and enter the following URL: http://<webservername>:8080/xmppchat.jsp
4. To start a chat session, select a routepoint and click the **Start Chat** button.
5. Check that expected IM treatments from the contact center (such as comfort messaging) appear in the chat client.
6. Check that the contact presents to the agent.
7. Accept the IM contact on Agent Desktop, and type a response.
8. Verify that the response appears in the chat window on the Web browser.
9. On the Web browser, type a message in the **Chat** text box and click **Send**.
10. Verify that the response appears in the Agent Desktop.

11. Click the **End Chat** button to end the chat session.

Chapter 22: Mission Critical High Availability campus co-resident server commissioning

This section describes how to configure Mission Critical High Availability (HA) resiliency for a pair of co-resident Contact Center Manager Server (CCMS) and Communication Control Toolkit (CCT) servers in a campus SIP-enabled contact center environment that uses an Avaya Aura® Communication Manager and an Avaya Aura® Session Manager.

For information about configuring hot-standby or warm standby High Availability (HA) in an Avaya Communication Server 1000-based contact center or a contact center with an Avaya Aura® SIP Enablement Services (SES) server, see High Availability campus co-resident server commissioning on page 361.

Mission Critical High Availability campus overview:

In a co-resident CCMS and CCT server configuration, one co-resident server is the active server and one is the standby server. The active CCMS and CCT server actively processes scripts and contacts and records statistics. The standby server shadows the active server. The standby server copies all configuration changes made on the active server and monitors the active server status. If the active server fails, the standby server, running in Mission Critical standby mode, recognizes the failure and starts processing contacts. After the switchover, High Availability is disabled on the original active server.

The active and standby co-resident CCMS and CCT servers are part of the same Avaya Aura® Contact Center and they must be in the same subnet IP address range for campus High Availability resiliency to work.

The standby server must be configured the same as the active server. The standby and active servers must have the same patch level and the same hard disk drive partitions. Configuration changes made to the active CCMS and CCT server during normal operation are automatically copied to the standby server so that the standby server can take over processing from the active server when necessary.

In a Mission Critical campus co-resident High Availability solution, a CCMS or CCT service failure, hardware, network, or database failure can initiate a switchover but only in the following situations:

- The active server is in the active mode.
- The active server is running. All the critical CCMS and CCT services are monitored and running.
- The active server has Enable Switchover enabled.
- The active and standby servers can communicate with the trusted server.
- The active server database and standby server database are synchronized. The standby server database is shadowing the active server database.

If the Contact Center Administrator uses the Windows Service Control Manager (SCM) to stop a monitored service on an Active server, a switchover occurs. If the Contact Center Administrator uses the System Control and Monitor Utility (SCMU) to stop a monitored service on an Active server, a switchover does not occur.

If a critical service on the Standby server stops or is stopped, the Standby server stops all services and the contact center solution is no longer resilient. To reinstate High Availability resiliency, use SMMC to “Start HA System” on the Standby server.

High Availability Utility:

Configure High Availability resiliency for CCMS and CCT using the High Availability (HA) Utility in the Database Utilities. The High Availability Utility is used to configure which server is the active and which is the standby server. The HA utility also configures the Managed IP of the active server.

The High Availability Utility on an Active Server has the following dialogs under the Configuration tab:

- Server Mode
  - Configure the IP address for the Active and Standby servers
  - Configure the IP address for Trusted servers
  - Configure the IP address for the optional Remote Geographic Node
  - Identify if the server is Active or Standby
  - Enable Switchover
  - Configure the switchover time-out. This is the wait time if a network outage occurs before an automatic switchover occurs
- Notifications
  - Configure an e-mail server for e-mail notifications
  - Configure where and how often to send e-mail notifications
  - Configure the e-mail character set
- System
  - Display information on the system status
  - Verify that database shadowing is running

SMMC system tray:

The Contact Center System Management and Monitoring Component (SMMC) system tray gives quick access to action items in your High Availability environment, for example:

- Start HA System
- Stop HA System
- Disable Switchover
- Enable Switchover

- System Information
- Database Information
- Disable Next Auto Startup
- Select Standby Auto Startup Mode (Standby server only)

To access the SMMC system tray menu, right-click the SMMC icon on the Windows taskbar.

High Availability Utility and SMMC system tray:

Use the High Availability Utility to configure High Availability IP addresses and to configure which server is the active server and which is the standby server. Then use the System Management and Monitoring Component (SMMC) system tray to start database shadowing and High Availability functionality.

Determining the High Availability Network Timeout threshold:

The level of Contact Center application High Availability you achieve depends on your complete enterprise contact center solution, including the underlying network infrastructure.

It is important that you determine the optimum High Availability SMMC Network Timeout threshold value for your contact center network. If the threshold is set too high, High Availability may not recognize network outages, switchover may not occur when necessary and call control may be lost. If the threshold is set too low, frequent and unnecessary switchovers may occur.

SMMC tests network connectivity between High Availability components and records the details of these connectivity tests in trace log files. The SMMC trace log files contain sufficient statistical data about SMMC communications in your network to characterize the networks behavior for a High Availability contact center solution. You can use this SMMC statistical communications data to optimize your High Availability solution.

Avaya recommends that you analysis the SMMC trace log file and use the connectivity test results in it to optimize the High Availability settings for your network. For more information about optimizing your High Availability configuration settings to your network, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).

To commission CCMS, CCT and CCMA see the following sections in this document:

- Contact Center Manager Server commissioning, see Contact Center Manager Server commissioning on page 33
- Contact Center Manager Administration commissioning, see Contact Center Manager Administration commissioning on page 121
- Communication Control Toolkit commissioning, see Communication Control Toolkit commissioning for Contact Center on page 219

Prerequisites

- Ensure the Avaya Aura® Unified Communications platform is installed and patched to support Avaya Aura® Contact Center High Availability.
- The active and standby servers must meet the planning and engineering specifications. For more information, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Ensure unused Network Interface Cards (NICs) are disabled.
- CCMS is installed on the Active and Standby servers using the same drive specification on each server. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCT is installed on the Active and Standby servers using the same drive specification on each server. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCMA is installed on the Active and the Standby servers. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCMA AD-LDS replication is configured. CCMA AD-LDS replication is configured at install time. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCMS is configured on the Active Server. For more information, see Contact Center Manager Server commissioning on page 33.
- CCT is configured on the Active Server. For more information, see Communication Control Toolkit commissioning for Contact Center on page 219.
- CCMA is configured on the Active Server. For more information, see Contact Center Manager Administration commissioning on page 121.
- License Manager is installed on the Active and the Standby Server. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- The Active and Standby Server have a valid standby server license file.
- Ensure the Communication Control Toolkit server is on a domain. This is to allow the CCT clients such as Avaya Aura® Agent Desktop to communicate with both CCT servers.
- Ensure CCMS, CCT and CCMA are commissioned on the active server.
- Ensure that the active Contact Center Manager Server is added as a CCMS type server in the primary CCMA - “Server Properties” page. For more information, see Adding the Contact Center Manager Server to Contact Center Manager Administration on page 149.

- Ensure that the active Communication Control Toolkit is added as a CCT type server in the primary CCMA - “Server Properties” page. For more information, see Adding the CCT Server in CCMA on page 216.
- Commission the Switchover Handling script. For more information about the Switchover Handling script, see *Avaya Aura® Contact Center Fundamentals* (NN44400-110).
- Before you commission High Availability, use System Control and Monitoring Utility (SCMU) to shut down all CCMS and CCT services on both the active and standby servers.

Mission Critical High Availability campus server commissioning procedures

About this task

This task flow shows the sequence of procedures to commission Mission Critical High Availability campus servers.

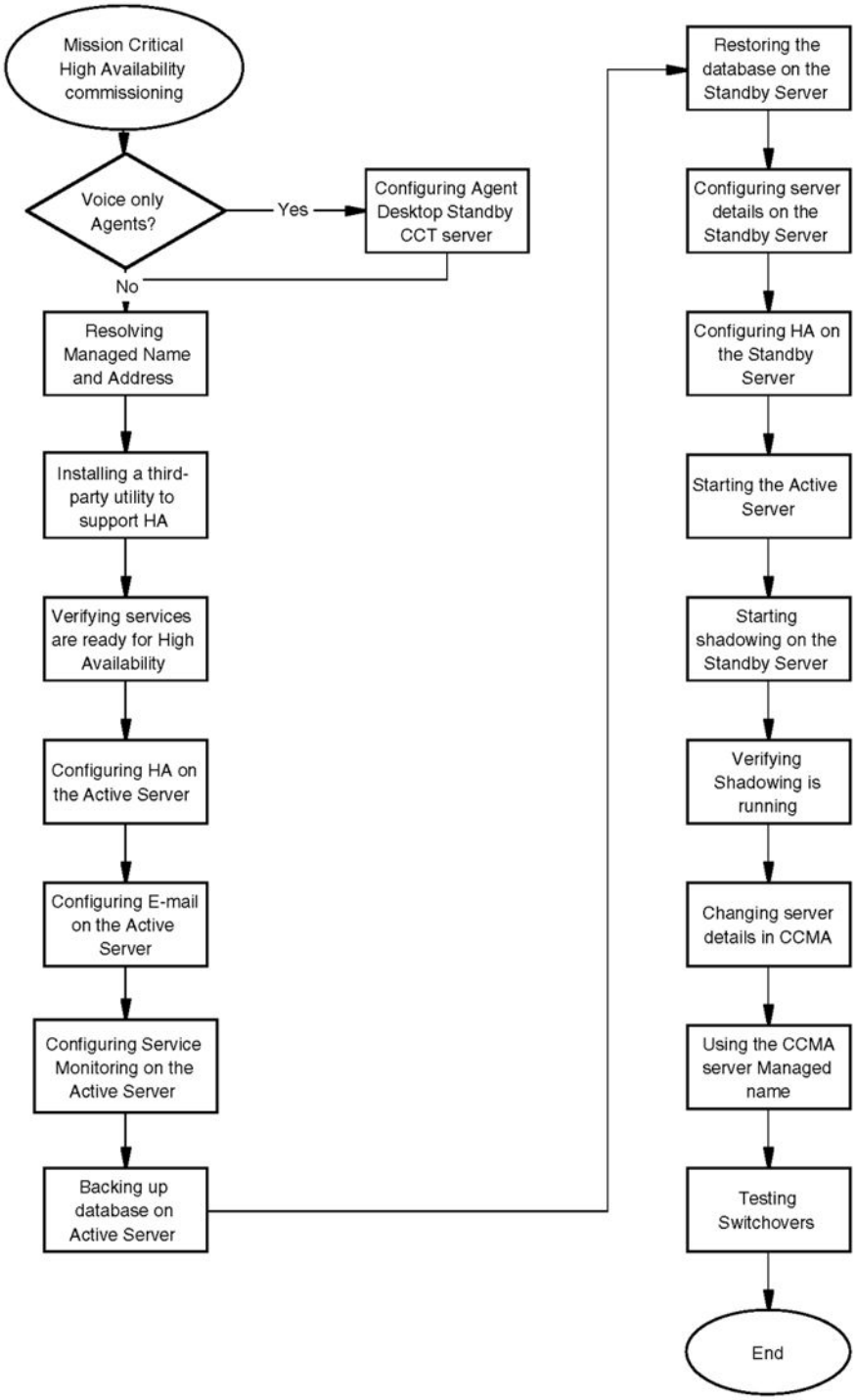


Figure 46: Mission Critical High Availability campus server commissioning procedures

Configuring Agent Desktop Standby CCT server

About this task

In a voice-only campus High Availability solution use the Agent Desktop Telephony Toolbar configuration utility to configure a standby Communication Control Toolkit (CCT) server.

In a multimedia-enabled solution Avaya Aura® Agent Desktop client software is typically downloaded from a Contact Center Multimedia (CCMM) server. Avaya Aura® Agent Desktop then communicates with that Contact Center Multimedia server to handle e-mail based contacts, and with a Communication Control Toolkit server to handle voice contacts.

In a multimedia-enabled High Availability solution use the CCMM Administration tool to configure standby CCMS and CCT server details. Avaya Aura® Agent Desktop client software downloads these standby server details and communicates with these standby servers if it cannot communicate with the active CCMM or CCT servers. For more information about configuring standby CCMM and CCT server details, see Configuring CCMM General Administration on page 423.

A voice-only campus High Availability solution has two CCT servers, an Active CCT server and a Standby CCT server. The Standby CCT server name or IP address is stored in a configuration file on the Active CCT server. Use the Agent Desktop Telephony Toolbar configuration utility to edit this file and configure the Agent Desktop Standby CCT server name or IP address.

In a voice-only contact center the Avaya Aura® Agent Desktop client software is downloaded from the Agent Desktop Telephony Toolbar on the Active CCT server. Under normal operation Agent Desktop connects to the Active CCT server and downloads the name of the Standby CCT server. Agent Desktop then authenticates with both CCT servers and uses the Active CCT server to handle voice contacts. If the Agent Desktop client software is unable to communicate with the Active CCT server it switches over and uses the Standby CCT server to handle voice contacts.

Procedure

1. Log on to the Active Communication Control Toolkit Server.
2. Navigate to <Installed Drive>:\Avaya\Contact Center\Multimedia Server\Agent Desktop\.
3. Double-click on **CCADConfigurator.exe** to start the Agent Desktop Toolbar configuration utility.
4. On the password message box, type the password. The default password is “ __avaya”.
5. Click **OK**.
6. On the **App Settings** tab, in the **CCTBackupServer** row and in the **Value** column, type the name of the Standby CCT server.

7. Click **Save**.
8. Click **OK**.

Resolving the Managed name to the Managed IP Address

About this task

Complete the following procedure on the Active and Standby servers to resolve the Managed server name to the Managed IP address using the Windows hosts file. If the server has two network interfaces, apply these settings to the CLAN network interface. Each Contact Center server in a domain requires a DNS static entry.

Important:

Avaya Aura® Contact Center High Availability solutions do not support Windows Server 2008 Dynamic DNS.

Ask your System Administrator to add a Domain Name System (DNS) static entry for the Active and Standby servers and one additional DNS static entry for the each Managed name and associated Managed IP address.

A typical High Availability campus solution with a pair of co-resident servers requires 3 DNS static entries; one DNS static entry for the active server, one DNS static entry for the standby server, and one DNS static entry for the Managed name and associated IP address.

Perform this procedure on the Active and Standby servers.

Procedure

1. Open Windows Explorer.
2. Go to the folder C:\Windows\system32\drivers\etc.
3. Double-click on the **hosts** file, select **Open**, and select **Notepad**.
   The hosts file opens in Notepad.
4. Add the Managed IP address and the Managed server name to the hosts file.

   Important:

   The Managed Server name can be a full name or netbios server name.

Installing a third-party utility to support High Availability

About this task

Install a third-party utility required by the Avaya Aura® Contact Center High Availability feature.

Perform this procedure on the Active and Standby servers.

Procedure

1. Log on to the Active Server.
2. Using Windows Explorer, navigate to <installation drive>:\Avaya\Contact Center \Manager Server\CCSMMC\thirdparty\winpcap.
3. Double-click **WinPcap_4_1_2.exe**.
4. On the WinPcap installer dialog, click **Next**.
5. On the WinPcap installer **Setup Wizard** dialog box, click **Next**.
6. On the WinPcap installer **License Agreement** dialog box, click **I Agree**.
7. On the WinPcap installer **Installation options** dialog box, click **Install**.
8. On the WinPcap installer dialog, click **Finish**.
9. Repeat this procedure on the Standby Server.

Verifying services are ready for High Availability

About this task

Verify that all CCMS and CCT services stop before you configure High Availability. This ensures that all resources are available to the Active Server when it starts.

Perform this procedure using the System Management and Monitoring Component (SMMC) on the Active and Standby servers.

Procedure

1. Log on to the Active Server.
2. On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Stop System**.

3. Repeat this procedure on the Standby Server.

Configuring High Availability on the Active Server

About this task

Configure High Availability resiliency on the Active Server using the High Availability Utility. The Active Server is the co-resident CCMS and CCT server that normally processes calls.

Procedure

1. Select one co-resident CCMS and CCT server to be the active server and log on.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.
4. Double-click **Server Mode**.
5. Under **Server Mode**, select **Active**.
6. Under **Switchover And Network Timeout Configuration**, select **Enable Switchover**.
7. Under **Switchover And Network Timeout Configuration**, in the **Network Timeout** box, type the maximum length of time the network connectivity tests can continue to fail consecutively before corrective action is considered.
8. Under **Switchover And Network Timeout Configuration**, from the drop down list, select the unit of time for the network connectivity tests.
9. Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the active server.
10. Under **IP Configuration**, in the **Standby CLAN** box, type the IP address for the standby server.
11. Under **IP Configuration**, in the **Managed IP** box, type the managed IP address.
12. Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server.
13. In the **Remote Geographic Node (Optional)** box, type the IP address of the optional Remote Geographic Node.
14. Under **SMMC Port Configuration**,in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the local (active) server.

15. Under **SMMC Port Configuration**,in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the remote (standby) server.
16. Click **OK**.

Variable definitions

Name	Description
Network Timeout	The High Availability feature tests network connectivity between HA components by default every 100 milliseconds (100ms). The High Availability—Network Timeout value sets the maximum length of time these network connectivity tests can continue to fail consecutively before corrective action is considered. For example, if Network Timeout is set to 400ms, HA requires 4 consecutive failed network connectivity tests before the remote system is marked as unreachable. In this case, if switchovers are enabled, an attempt to switch over is made. Avaya recommends that you set Network Timeout high enough to be tolerant of normal network latency, but low enough to be responsive if a failure occurs.
Active CLAN	The IP address for the server initially configured in Active mode.
Standby CLAN	The IP address for the server initially configured in Standby mode.
Managed IP	The virtual Managed IP (MIP) address that is used by the Active Server for campus resiliency. A MIP is used only when the Active and Standby servers are in the same subnet.
Trusted IP	The Active and Standby servers use the Trusted IP address to verify network connectivity. If the Active server cannot communicate with the Standby server it attempts to communicate with the Trusted IP address. If the Active server cannot communicate with the Trusted IP address, if shadowing and switchover are enabled, then

Name	Description
	the Active server stops processing contacts and shuts down. The Standby server starts processing contacts if it cannot communicate with the Active server but can communicate with the Trusted IP address. Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
Remote Geographic Node (Optional)	The IP address of the optional Remote Geographic Node.
Local SMMC Port	The port number for System Management and Monitoring Component (SMMC) on the local (active) server. The default port number is 57012.
Remote SMMC Port	The port number for System Management and Monitoring Component (SMMC) on the remote (standby) server. The port number entered here must match the port number set on the remote (standby) server. The default port number is 57012.

Procedure job aid

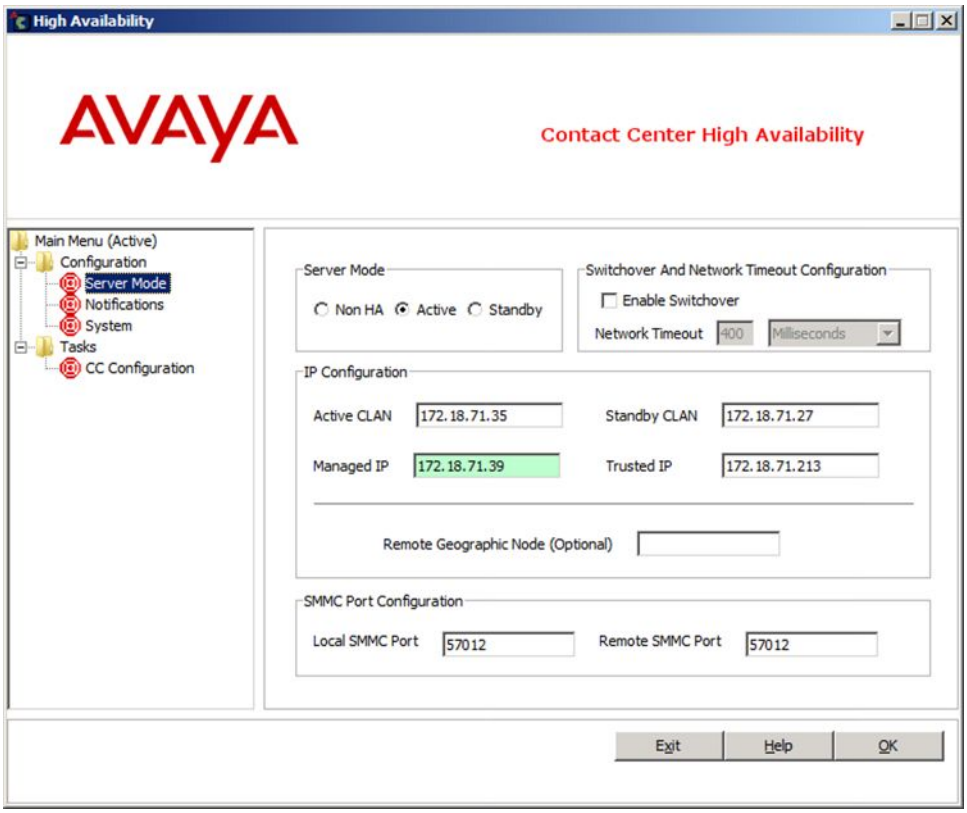


Figure 47: Example of configuring Mission Critical High Availability on an active server

Configuring E-mail notification on the Active Server

Before you begin

- If anonymous users are allowed, a user name and password may not be required. Check with the Administrator of the e-mail server for setup configuration.

About this task

If an automatic switchover occurs, the High Availability utility can send e-mail messages to configured users at a defined interval.

The default e-mail notification character set is US_ASCII. The following character sets are also supported:

- ISO-8859-1
- UTF-8

- UTF-16BE
- UTF-16LE
- UTF-16

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.
4. Double-click **Notification**.
5. Select the **Email** check box.
6. Type the **SMTP Server** name.
7. Type the **Username**.
8. Type the **Password**.
9. Type the **From Address**.
10. Type the **To Address** or **Addresses**.
11. Click **OK** to save the data.

Variable definitions

Name	Description
Email	Enables or disables e-mail notifications.
SMTP Server	The SMTP Server name, which is automatically verified when saving the data.
Username	E-mail User log on name.
Password	E-mail User log on 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.

Configuring service monitoring on the Active Server

About this task

The High Availability feature monitors a number of critical services on the Active Server. If these critical services stop or fail, they automatically restart in the correct order. If a critical service fails a defined number of times, the Active Server may, if Switchover is enabled, shut down and hand over processing to the Standby Server.

Critical services are listed, monitored, restarted, and controlled using the Contact Center Configuration tab on the Tasks tab of the High Availability utility. The Contact Center Configuration tab lists the critical CCMS services and all of the CCT services on the co-resident 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 occurs.

For switchover to occur, both the Active and the Standby servers must have their respective switchover check box 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 RestartThreshold is the time period within when the services are monitored and the counters are increased when services fail. When this threshold is met, the counters are reset to zero, monitoring restarts, and the restart threshold timer resets.

⚠ Caution:

The default CCT services *Start Wait Time* is 60 seconds. Do not configure the CCT services *Start Wait Time* to be less than 60 seconds.

Procedure

1. Log on to the Active Server.
2. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. In the High Availability window, in the left pane, expand the **Tasks** folder.
4. Double-click **CC Configuration**.
5. For each service to monitor, select the **Monitor** check box.
6. For each service to restart, select the **Restart** check box.

Important:

By default service monitoring is selected for CCT and is not selected for CCMS.

7. In the **Start Wait Time** column, type the number of seconds to wait before restarting a service.
8. For CCT only, in the **Stop Wait Time** column, type the number of seconds to wait before stopping a service.
9. In the **Restart Limit** column, type the maximum number of attempts to restart the service before switchover occurs.This Administrator decides the maximum number.
10. In the **Restart Threshold** column, type the time in seconds to reset the restart counter (for each service that is restarted) after the threshold is passed.

Variable definitions

Name	Description
CC	The Contact Center application name, CCMS or CCT in this case, because CCMS and CCT are co-resident.
Service	The application service name, for example OAM_Service.
Monitor	Used to enable or disable the service monitoring.
Restart	Restart the service if it stops.
Start Wait Timer	The time in seconds that service monitor waits before attempting to restart or initiating a switchover to the standby server if this service is not running. The default CCT services *Start Wait Time* is 60 seconds. Do not configure the CCT services *Start Wait Time* to be less than 60 seconds.
Stop Wait Time	The waiting time (in seconds) for the next restart decision. For example, if service monitor stopped this service, service monitor checks the status if the status is not SERVICE_STOPPED, it waits for Stop Wait Time before attempting to start the service.

Name	Description
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.

Procedure job aid

This section provides an example of the service monitor configuration in the High Availability Utility.

When the CCMS OAM service has stopped 3 times for longer than 60 seconds in a period of 12 hours, initiate an automatic switchover. This requirement is achieved by setting the OAM service configuration values to the following settings:

CC	CCMS
Service	OAM_Service
Monitor	Selected
Restart	Selected
Start Wait Timer	60 Seconds
Restart Limit	3
Restart Threshold	43200 Seconds (12 hours)

Backing up the database on the Active Server

About this task

The Active Server is configured for High Availability. Now the Standby Server must be prepared for High Availability resiliency. Back up the Active Server to create a snapshot of the database which is then restored to the Standby Server. On the active co-resident server all databases must be backed-up.

Important:

You must backup the Active server database, restore it onto the Standby server, and enable shadowing within 24 hours. If the difference in time between the Active and Standby server database content is greater than 24 hours then database shadowing does not work. If

shadowing is stopped for more than 24 hours then you must backup the Active server database and restore it onto the Standby server before re-enabling shadowing. Ensure that the system clock time on the Active and Standby servers are synchronized.

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
3. Click **Backup Locations**.
4. Click **Create**.
5. From the **Driver Letter** list, select the network drive on which you want to store the Contact Center Manager Server, CCT and ADMIN databases.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Backup Location. This location must be a shared folder with correct permissions.

   Important:

   If your contact center includes Contact Center Multimedia as a standalone server, do not use the same backup folder for your co-resident and multimedia ADMIN databases, as ADMIN databases stored in the same backup location overwrite each other.
7. In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the Windows password.
9. Click **OK**.
10. In the left pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Disk**.
12. In the **Applications** section, select **CCMS**, **CCT** and **ADMIN**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.

Restoring the database on the Standby Server

Before you begin

- Know the location of the backup database. Copy the database backups onto the Standby server.
- Ensure no traffic is running on the Standby Server.
- Stop shadowing if shadowing is running on the Standby Server.
- Stop all Contact Center services using the SCMU utility, if services are running.
- Ensure the patch level on the Standby Server is the same as the Active Server.

Important:

Not all CCT data is stored in the database; therefore the following data must be configured on the Standby Server, CCT License, CCT Contact Management Framework, CCT SOA configuration and CCT logging location. For information about CCT commissioning, see Communication Control Toolkit commissioning for Contact Center on page 219.

Important:

You must restore all databases in a co-resident server. Restoring only CCMS and not CCT or ADMIN may leave an inconsistent server and HA cannot shadow data correctly.

Important:

Restoring the Admin database can change configuration of Backup locations on the Standby Server if the Active Server and Standby Server backup locations are different. Therefore, after you restore the ADMIN database, close and reopen the Database and Maintenance utility.

Important:

The Server Configuration utility must be run after a database restore has been performed and the administrator must check the data to ensure that it is correct.

About this task

Restore the database from the Active Server to the Standby Server to ensure the databases are consistent. The Database Maintenance utility can restore only one application database at a time. Restore the data for the CCMS, CCT, and ADMIN databases

You must restore the CCMS, CCT, and ADMIN database onto the Standby Server. You must restore the ADMIN database last.

Important:

You must backup the Active server database, restore it onto the Standby server, and enable shadowing within 24 hours. If the difference in time between the Active and Standby server

database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the Active server database and restore it onto the Standby server before re-enabling shadowing. Ensure that the system clock time on the Active and Standby servers are synchronized.

Procedure

1. Log on to the Standby Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
3. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
4. In the right pane, under **Media Type**, select the media type on which the backup is restored.
5. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
6. Under **Application**, select the database to restore, either CCMS, CCT or ADMIN.
7. Under **Restore contents**, select Data.
8. Click **Restore**.
9. Use the **Progress information** field to monitor the progress of the restoration.
10. Repeat steps 6 to 8 to restore all databases.
11. Click **Exit** to close the Database Maintenance utility.

Variable definitions

Name	Description
Application	The database and applications of Contact Center that you can back up.
Backup Location	The destination of the network disk. The values are configured in the Backup Locations.
Restore contents	The type of content that is stored in the database. Data is in the database. Schema is the data for the database structure, tables and procedures.
Media type	The type of media used for your backup file. You can use a network disk location or a tape drive.

Name	Description
	If you use a network disk location, you must configure a destination before you can back up the file.

Configuring server details on the Standby Server

Before you begin

- The Active Server databases are restored on to the Standby Server.

About this task

After you restore the Active Server database on to the Standby Server, the Standby Server database contains the same agent and statistical data as the Active Server. However the Standby Server server details are now also configured exactly the same as the Active Server, therefore you must reconfigure the Standby Server with its own server details.

Important:

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

Procedure

1. Log on to the Standby Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
3. In the **Server Configuration** dialog box, click the **Local Settings** tab.
4. Update the Standby Server local settings.
5. Click **Apply All**.
6. In the **Server Configuration** dialog box, click the **Licensing** tab.
7. Update the Standby Server licensing details.
8. Click **Apply All**.
9. Click **OK**.
10. In the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.
11. Update the Standby Server **SIP Network Settings** details.
12. Click **Apply All**.

13. Click **OK**.
14. In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.
15. Update the Standby Server **SIP Local Subscriber** details.
16. Click **Apply All**.
17. Click **OK**.
18. Click **Exit**.

Variable definitions

Name	Description
Avaya Server Subnet IP Address	The IP address of the subnet that connects the Contact Center servers (Contact Center Manager Server, Network Control Center, Contact Center Manager Administration, and Contact Center Multimedia).
Voice Proxy Server • IP or FQDN • Port • Network Transport	Information about the server that provides support for inbound and outbound calls, such as routing a call to an agent telephone. If the contact center uses an Avaya Aura® Session Manager, enter the IP address or Fully Qualified Domain Name (FQDN) for the primary Session Manager. The server listening port. The default port is 5060. The SIP Network Transport communication protocol.
CTI Proxy Server • IP or FQDN • Port • Network Transport	Information about the server that provides support for SIP Computer Telephony Integration (CTI) so that Agent Desktop can acquire and control agent telephones for TR87. If the contact center uses an Avaya Aura® Application Enablement Services server, enter the IP address or Fully Qualified Domain Name (FQDN) for it. For an Application Enablement Services server the default SIP CTI Proxy Server port is 4723. The SIP Network Transport communication protocol.

Name	Description
	For an Application Enablement Services server, the default Network Transport communication protocol is TLS.
Backup Voice Proxy Server • IP or FQDN • Port • Network Transport	Information about the server that provides backup support for inbound and outbound calls, such as routing a call to an agent telephone. Avaya Aura® Contact Center must have a Standby Server license to support a Backup Voice Proxy Server. The only type of Backup Voice Proxy Server supported by Avaya Aura® Contact Center is an Avaya Aura® Session Manager when it used with an Avaya Aura® Communication Manager. If the contact center uses an Avaya Aura® Communication Manager and a backup Session Manager, enter the IP address or Fully Qualified Domain Name (FQDN) for the backup Session Manager. The server listening port. The default port is 5060. The Backup Voice Proxy Server transport protocol.
IM Proxy Server • IP or FQDN • Port • Network Transport	Information about the server that supports the deployment of Instant Message over SIP. From the IM Provider list, select the name of the instant messaging provider. Select either Aura Presence Services or Microsoft OCS. The IP address or Fully Qualified Domain Name (FQDN) of the SIP IM Proxy Server. The default SIP IM Proxy Server port is 5222. The IM SIP Proxy Server transport protocol.
IM Provider	Select your IM Provider, Microsoft OCS or Aura Presence Services.
XMPP Domain	If using an Avaya Aura® Presence Services server, enter the domain name of the Extensible Messaging and Presence Protocol (XMPP) server.
Local SIP Subscriber • Contact Center Name • Domain Name • Password	Information about the environment of the SIP-enabled contact center and how to identify the server within the network. The registration user name on the registration proxy. Use a suitable user name following the standards in your system.

Name	Description
	Associated domain name for the SIP-enabled contact center. Password for the registration user name.
Web Service Ports	The Web Service Ports group box appears only if you select Avaya Aura® Presence Services as the IM Provider. Server Port default is 9100 Client Port default is 9120
SIP Server Type	Type of SIP proxy for the contact center integration. Depending on the switch type you select in the Application Selection window, the system automatically sets the specific SIP Server Type as the default. • For SIP Avaya Aura® 6.1 switch type, the default SIP Server Type is Avaya Aura® 6.1.
MS Locale	Locale (including language and dialects) of the system environment.
Local Listening Ports	The SIP Communication protocol accepted by the system for incoming calls. TCP/UDP Port default is 5060 TLS Port default is 5061

Configuring High Availability on the Standby Server

Before you begin

- The Active Server databases are restored on to the Standby Server.

About this task

Configure High Availability resiliency on the Standby Server using the High Availability utility. The co-resident CCMS and CCT Standby Server shadows the Active Server and takes over processing if the Active Server fails.

Procedure

1. Log on to the Standby Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.

4. Double-click **Server Mode**.
5. Under **Server Mode**, select **Standby**.
6. Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the active server.
7. Under **IP Configuration,** in the **Standby CLAN** box, type the IP address for the standby server.
8. Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server.
9. Under **SMMC Port Configuration**,in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the remote (active) server.
10. Under **SMMC Port Configuration**,in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the local (standby) server.
11. Click **OK**.

Variable definitions

Name	Description
Active CLAN	The IP address for the server initially configured in Active mode.
Standby CLAN	The IP address for the server initially configured in Standby mode.
Managed IP	The virtual Managed IP (MIP) address that is used by the Active Server for campus resiliency. A MIP is used only when the Active and Standby servers are in the same subnet.
Trusted IP	The Active and Standby servers use the Trusted IP address to verify network connectivity. If the Active server cannot communicate with the Standby server it attempts to communicate with the Trusted IP address. If the Active Server cannot connect to the Trusted IP address on startup then no Contact Center services start on that server. If the Active server cannot communicate with the Trusted IP address, if shadowing and switchover are enabled, then the Active

Name	Description
	server stops processing contacts and shuts down. The Standby server starts processing contacts if it cannot communicate with the Active server but can communicate with the Trusted IP address. Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
Local SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the local (standby) server. The default port number is 57012.
Remote SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the remote (active) server. The port number entered here must match the port number set on the remote (active) server. The default port number is 57012.

Procedure job aid

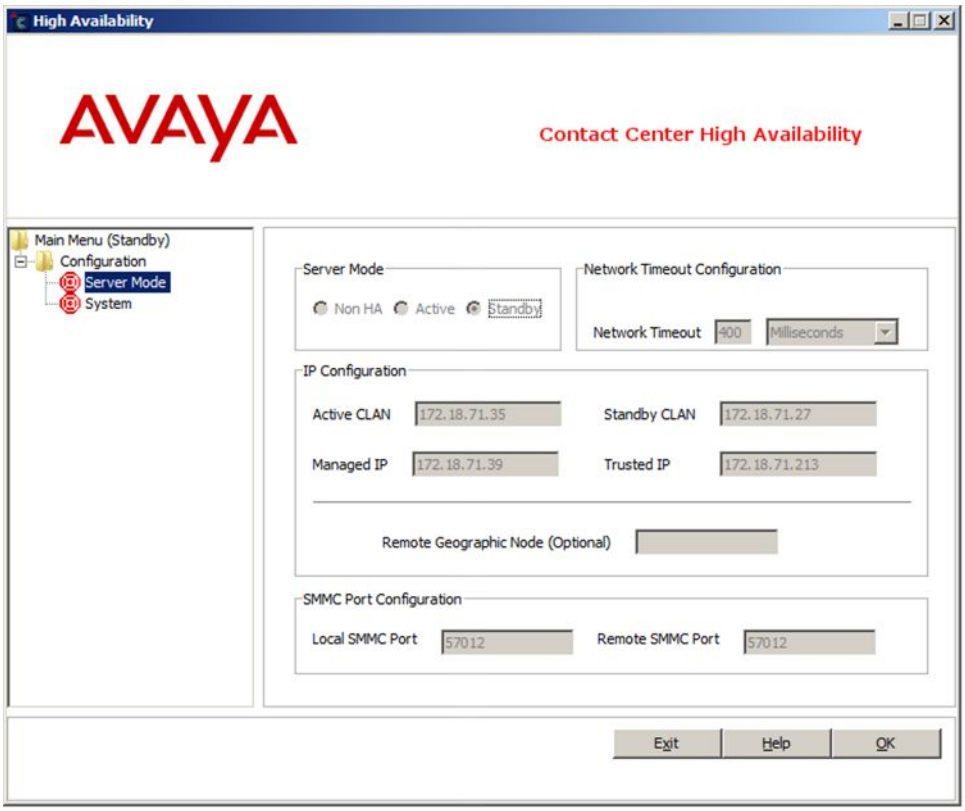


Figure 48: Example of configuring Mission Critical High Availability on a standby server

Starting the Active Server

About this task

Start the Active Server using the System Management and Monitoring Component (SMMC) system tray. Starting the Active Server starts CCMS, CCT, and system processes.

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.

4. Under **Switchover And Network Timeout Configuration**, select **Enable Switchover**.
5. Click **OK**.
6. On the Windows taskbar of the active server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**.
7. To verify that the Contact Center services are running using the SCMU, select **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**. Check the CCMS and CCT services are running.

Starting shadowing on the Standby Server

About this task

Start shadowing on the Standby Server using the System Management and Monitoring Component (SMMC) system tray.

The Standby co-resident CCMS and CCT server shadows the Active CCMS and CCT server, maintaining a near real-time local copy of the CCMS, CCT, and Administration databases. Therefore, the Standby Server is configured with the most recent data and it can take over from the Active Server if necessary.

Important:

You must backup the Active server database, restore it onto the Standby server, and enable shadowing within 24 hours. If the difference in time between the Active and Standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the Active server database and restore it onto the Standby server before re-enabling shadowing. Ensure that the system clock time on the Active and Standby servers are synchronized.

Procedure

1. Log on to the Standby Server.
2. On Windows taskbar of the standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**.
3. To verify that the Contact Center services are running using the SCMU, select **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**.Check the CCMS and CCT services are running.

Verifying High Availability is running on the Active Server

About this task

Verify that the Standby co-resident CCMS and CCT server is shadowing the Active server using the High Availability Utility. The System dialog box of the High Availability utility displays system information about the Active and the Standby servers.

The dialog box displays the followings information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information
- License information
- Databases shadowed
- Time of last record shadowed
- Database namespaces
- Local and remote information on system status, switchover, shadowing and network
- CC Application install information
- Database space and journaling information
- Database processes information

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. In the left pane, expand **Configuration**.
4. Select **System**.
5. Select **Get System Configuration**.
   The most recent system information appears.

Changing server details in Contact Center Manager Administration

About this task

In Contact Center Manager Administration, change the Contact Center Manager Server and Communication Control Toolkit server details to use the High Availability Managed IP address and Managed name details.

The High Availability Managed IP address and Managed name details entered here must match those configured in Resolving the Managed name to the Managed IP Address on page 312.

Procedure

1. Log on to the active server.
2. Log on to the Contact Center Manager Administration application with administrative privileges.
3. On the **Launchpad**, click **Configuration**.
4. From the list of servers in the system tree, right-click on the active CCMS server, and select **Edit Properties**.
5. In the **Server Name** box, type the High Availability Managed name of the Contact Center Manager Server.
6. In the **IP Address** box, type the High Availability Managed IP address of the Contact Center Manager Server.
7. In the **Display Name** box, type the name of the Contact Center Manager Server as you want it to appear in the system tree of Contact Center Administration.
8. Click **Submit**.
9. From the list of servers in the system tree, right-click on the active CCT server, and select **Edit Properties**.
10. In the **Server Name** box, type the High Availability Managed name of the Communication Control Toolkit server.
11. In the **IP Address** box, type the High Availability Managed IP address of the Communication Control Toolkit server.
12. In the **Display Name** box, type the name of the Communication Control Toolkit as you want it to appear in the system tree of Contact Center Administration.
13. Click **Submit**.

Using the Contact Center Manager Administration server Managed name

Before you begin

- Configure High Availability on the Active and Standby servers.
- Change the server details in CCMA. For more information about changing the server details in CCMA, see Changing server details in Contact Center Manager Administration on page 334.
- Know the user ID and password to log on to the CCMA.

About this task

Use the High Availability Managed name of the Contact Center Manager Administration server to access the CCMA application. When the Avaya Aura® Contact Center High Availability feature is configured and enabled, re-direct all Contact Center Manager Administration client Web browsers to use the Managed server name of the CCMA server.

If you have a High Availability campus co-resident solution Avaya recommends that you log on to the CCMA Web client using the Managed name of the co-resident CCMS and CCMA server. If an active application or server fails, the CCMA client Web browser continues to use the Managed name and you can continue working without interruption.

Important:

Do not type the real or Managed IP address in the Address box. Using an IP address results in problems with Scripting, Historical Reporting, Configuration, Contact Center Management, and Access and Partition Management.

Procedure

1. Start Internet Explorer.
2. In the **Address** box, type the URL of the CCMA server. The default URL is http://<*server name*>; where <*server name*> is the Managed server name of the CCMA server.
3. In the **User ID** box, type your user ID.
4. In the **Password** box, type your password.
5. Click **Login**.

Testing switchovers

Before you begin

- Configure High Availability on the Active and Standby servers.

About this task

Test the High Availability feature and infrastructure by making a manual switchover from the Active server to the Standby server.

Procedure

1. Log on to the current Active Server.
2. On the Windows taskbar, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Manual Switchover**.

Procedure job aid

When the Standby Server becomes the new Active Server, test the Standby Server configuration by making a call using the CCT Reference Client. For more details, see Verifying CCT using the Reference Client on page 235.

Chapter 23: High Availability Remote Geographic Node server commissioning

This section describes how to configure geographic High Availability resiliency for a pair of co-resident CCMS and CCT servers in an Avaya Aura® Communication Manager and an Avaya Aura® Session Manager Release 6.1 or Release 6.2 based contact center. Avaya Aura® Contact Center geographic High Availability supports data resiliency and Disaster Recovery.

For information about configuring geographic High Availability (HA) in an Avaya Communication Server 1000 based solution, see High Availability Geographic co-resident server commissioning on page 395.

In geographic Wide Area Network solutions the standby server on the remote geographic site is called a Remote Geographic Node server. The Active server and the Remote Geographic Node server are part of the same Avaya Aura® Contact Center solution but they are typically in different geographic locations and subnets.

To ensure no single point of failure in a Mission Critical High Availability solution, the Active server must also have a local Standby server in the same campus location. The Standby server shadows the Active server. If the Active server fails the local Standby server takes over call processing on the local site.

The Remote Geographic Node server on the remote site shadows the Active server on the campus site. If the Active server fails, the local Standby server assumes the shared Managed IP address and starts processing calls. The Remote Geographic Node server monitors the campus Managed IP address so it continues shadowing.

Remote Geographic Node server commissioning overview:

In a geographic co-resident CCMS and CCT server configuration, one server is the Active server and one is the Remote Geographic Node server. The active CCMS and CCT server actively processes scripts and contacts and records statistics. The Remote Geographic Node server shadows the active server. The Remote Geographic Node server copies all configuration changes made on the Active server and monitors the Active server status. The Remote Geographic Node server does not automatically take over if the active system fails. You must start the Remote Geographic Node server manually.

The Remote Geographic Node server must be configured the same as the active server. The Remote Geographic Node and Active servers must have the same patch level and the same hard disk drive partitions. Configuration changes made to the active CCMS and CCT server during normal operation are automatically copied to the Remote Geographic Node server by the shadowing process.

High Availability Utility:

Configure High Availability resiliency for CCMS and CCT using the High Availability (HA) Utility in the Database Utilities. The High Availability Utility is used to configure which server is the active and which is the Remote Geographic Node (standby) server. The HA utility also configures the Managed IP of the active server.

The High Availability Utility on an Active Server has the following dialogs under the Configuration tab:

- Server Mode
  - Configure the IP address for the Active and Standby servers
  - Configure the IP address for Trusted servers
  - Configure the IP address for the optional Remote Geographic Node
  - Identify if the server is Active or Standby
  - Enable Switchover
  - Configure the switchover time-out. This is the wait time if a network outage occurs before an automatic switchover occurs
- Notifications
  - Configure an e-mail server for e-mail notifications
  - Configure where and how often to send e-mail notifications
  - Configure the e-mail character set
- System
  - Display information on the system status
  - Verify that database shadowing is running

SMMC system tray:

The Contact Center System Management and Monitoring Component (SMMC) system tray gives quick access to action items in your High Availability environment, for example:

- Start HA System
- Stop HA System
- Disable Switchover
- Enable Switchover
- System Information
- Database Information

To access the SMMC system tray menu, right-click the SMMC icon on the Windows taskbar.

High Availability Utility and SMMC system tray:

Use the High Availability Utility to configure High Availability IP addresses and to configure which server is the active server and which is the standby server. Then use the System Management and Monitoring Component (SMMC) system tray to start database shadowing and High Availability functionality.

To commission CCMS, CCT and CCMA see the following sections in this document:

- Contact Center Manager Server commissioning, see Contact Center Manager Server commissioning on page 33
- Contact Center Manager Administration commissioning, see Contact Center Manager Administration commissioning on page 121
- Communication Control Toolkit commissioning, see Communication Control Toolkit commissioning for Contact Center on page 219

Prerequisites

- The active, standby, and Remote Geographic Node servers must meet the planning and engineering specifications. For more information, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Ensure unused Network Interface Cards (NICs) are disabled.
- CCMS is installed on the Active, Standby, and Remote Geographic Node servers using the same drive specification on each server. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCT is installed on the Active, Standby, and Remote Geographic Node servers using the same drive specification on each server. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCMA is installed on the Active, Standby, and the Remote Geographic Node servers. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCMA replication is configured. CCMA Replication is setup at install time. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCMS is configured on the Active and Standby Servers. For more information, see Contact Center Manager Server commissioning on page 33.
- CCT is configured on the Active and Standby Servers. For more information, see Communication Control Toolkit commissioning for Contact Center on page 219.
- CCMA is configured on the Active Server. For more information, see Contact Center Manager Administration commissioning on page 121.
- The active and standby servers in the High Availability campus site are installed and commissioned. Remote Geographic Node servers are supported only when the High Availability campus site has both an Active server and a Standby server.
- License Manager is installed on the Active and the Remote Geographic Node server. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- Have a valid standby server license file on the Active and Remote Geographic Node server.

- Ensure the Communication Control Toolkit server is on a domain. This is to allow the CCT clients to automatically re-connect after a switchover.
- Before you commission High Availability, use System Control and Monitoring Utility (SCMU) to shut down all CCMS and CCT services on both the active and Remote Geographic Node servers.

High Availability Remote Geographic Node server commissioning procedures

About this task

This task flow shows the sequence of procedures to commission High Availability Geographic servers.

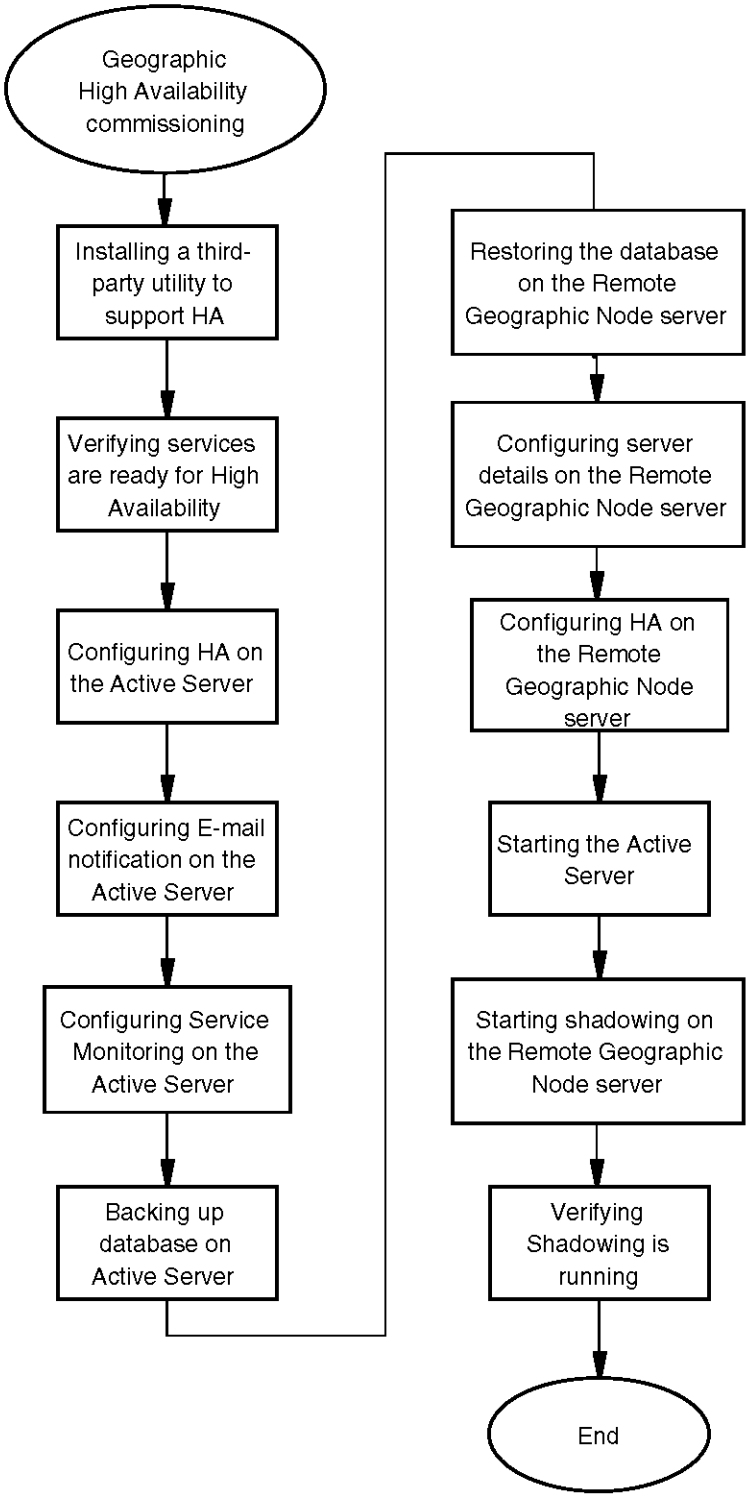


Figure 49: High Availability Remote Geographic Node server commissioning procedures

Installing a third-party utility to support High Availability

About this task

Install a third-party utility required by the Avaya Aura® Contact Center High Availability feature.

Perform this procedure on the Active and Remote Geographic Node servers.

Procedure

1. Log on to the Active Server.
2. Using Windows Explorer, navigate to <installation drive>:\Avaya\Contact Center \Manager Server\CCSMMC\thirdparty\winpcap.
3. Double-click **WinPcap_4_1_2.exe**.
4. On the WinPcap installer dialog, click **Next**.
5. On the WinPcap installer **Setup Wizard** dialog box, click **Next**.
6. On the WinPcap installer **License Agreement** dialog box, click **I Agree**.
7. On the WinPcap installer **Installation options** dialog box, click **Install**.
8. On the WinPcap installer dialog, click **Finish**.
9. Repeat this procedure on the Remote Geographic Node Server.

Verifying services are ready for High Availability

About this task

Verify that all CCMS and CCT services stop before you configure High Availability. This ensures that all resources are available to the Active Server when it starts.

Perform this procedure using the System Management and Monitoring Component (SMMC) on the Active server.

Procedure

1. Log on to the Active Server.
2. On the Windows System Tray, right-click on the System Management and Monitoring Component (SMMC) system tray icon, and select **Stop System**.

Configuring High Availability on the Active Server

About this task

Configure High Availability resiliency on the Active Server using the High Availability Utility. The Active Server is the co-resident CCMS and CCT server that normally processes calls.

Procedure

1. Select one co-resident CCMS and CCT server to be the active server and log on.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.
4. Double-click **Server Mode**.
5. Under **Server Mode**, select **Active**.
6. Under **Switchover And Network Timeout Configuration**, in the **Network Timeout** box, type the maximum length of time the network connectivity tests can continue to fail consecutively before corrective action is considered.
7. Under **Switchover And Network Timeout Configuration**, from the drop down list, select the unit of time for the network connectivity tests.
8. Under **IP Configuration**, in the **Active CLAN** box, type the IP address for the active server.
9. Under **IP Configuration**, in the **Standby CLAN** box, type the IP address for the standby server.
10. Under **IP Configuration**, in the **Managed IP** box, type the managed IP address.
11. Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server.
12. In the **Remote Geographic Node (Optional)** box, type the IP address of the Remote Geographic Node.
13. Under **SMMC Port Configuration**,in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the local (active) server.
14. Under **SMMC Port Configuration**,in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the remote (standby) server.
15. Click **OK**.

Variable definitions

Name	Description
Network Timeout	The High Availability feature tests network connectivity between HA components by default every 100 milliseconds (100 ms). The High Availability—Network Timeout value sets the maximum length of time these network connectivity tests can continue to fail consecutively before corrective action is considered. For example, if Network Timeout is set to 400 ms, HA requires 4 consecutive failed network connectivity tests before the remote system is marked as unreachable. In this case, if switchovers are enabled, an attempt to switchover is made. Avaya recommends that you set Network Timeout high enough to be tolerant of normal network latency, but low enough to be responsive if a failure occurs.
Active CLAN	The IP address for the server initially configured in Active mode.
Standby CLAN	The IP address for the server initially configured in Standby mode.
Managed IP	The virtual Managed IP (MIP) address that is used by the Active Server for campus resiliency. A MIP is used only when the Active and Standby servers are in the same subnet.
Trusted IP	Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
Remote Geographic Node (Optional)	The IP address of the Remote Geographic Node.
Local SMMC Port	The port number for System Management and Monitoring Component (SMMC) on the local (active) server. The default port number is 57012.
Remote SMMC Port	The port number for System Management and Monitoring Component (SMMC) on the

Name	Description
	remote (standby) server. The port number entered here must match the port number set on the remote (standby) server. The default port number is 57012.

Configuring E-mail notification on the Active Server

Before you begin

- If anonymous users are allowed, a user name and password may not be required. Check with the Administrator of the e-mail server for setup configuration.

About this task

If an automatic switchover occurs, the High Availability utility can send e-mail messages to configured users at a defined interval.

The default e-mail notification character set is US_ASCII. The following character sets are also supported:

- ISO-8859-1
- UTF-8
- UTF-16BE
- UTF-16LE
- UTF-16

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.
4. Double-click **Notification**.
5. Select the **Email** check box.
6. Type the **SMTP Server** name.
7. Type the **Username**.
8. Type the **Password**.
9. Type the **From Address**.
10. Type the **To Address** or **Addresses**.

11. Click **OK** to save the data.

Variable definitions

Name	Description
Email	Enables or disables e-mail notifications.
SMTP Server	The SMTP Server name, which is automatically verified when saving the data.
Username	E-mail User log on name.
Password	E-mail User log on 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.

Configuring service monitoring on the Active Server

About this task

The High Availability feature monitors a number of critical services on the Active Server. If these critical services stop or fail, they automatically restart in the correct order.

Critical services are listed, monitored, restarted, and controlled using the Contact Center Configuration tab on the Tasks tab of the High Availability utility. The Contact Center Configuration tab lists the critical CCMS services and all of the CCT services on the co-resident CCMS and CCT server.

There is no requirement to change the data in this table, the default values are suitable for most solutions.

The RestartThreshold is the time period within when the services are monitored and the counters are increased when services fail. When this threshold is met, the counters are reset to zero, monitoring restarts, and the restart threshold timer resets.

Procedure

1. Log on to the Active Server.
2. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. In the **High Availability** window, in the left pane, expand the **Tasks** folder.

4. Double-click **CC Configuration**.
5. For each service to monitor, select the **Monitor** check box.
6. For each service to restart, select the **Restart** check box.

   Important:

   By default service monitoring is selected for CCT and is not selected for CCMS.
7. In the **Start Wait Time** column, type the number of seconds to wait before restarting a service.
8. For CCT only, in the **Stop Wait Time** column, type the number of seconds to wait before stopping a service.
9. In the **Restart Limit** column, type the maximum number of attempts to restart the service before switchover occurs.This Administrator decides the maximum number.
10. In the **Restart Threshold** column, type the time in seconds to reset the restart counter (for each service that is restarted) after the threshold is passed.

Variable definitions

Name	Description
CC	The Contact Center application name, CCMS or CCT in this case, because CCMS and CCT are co-resident.
Service	The application service name, for example OAM_Service.
Monitor	Used to enable or disable the service monitoring.
Restart	Restart the service if it stops.
Start Wait Timer	The time in seconds that service monitor waits before attempting to 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. For example, if service monitor stopped this service, service monitor checks the status if the status is not SERVICE_STOPPED, it waits for Stop Wait Time before attempting to start the service.

Name	Description
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.

Procedure job aid

This section provides an example of the service monitor configuration in the High Availability Utility.

When the CCMS OAM service has stopped 3 times for longer than 60 seconds in a period of 12 hours, initiate an automatic switchover. This requirement is achieved by setting the OAM service configuration values to the following settings:

CC	CCMS
Service	OAM_Service
Monitor	Selected
Restart	Selected
Start Wait Timer	60 Seconds
Restart Limit	3
Restart Threshold	43200 Seconds (12 hours)

Backing up the database on the Active Server

About this task

The Active Server is configured for High Availability. Now the Remote Geographic Node server must be prepared for High Availability resiliency. Back up the Active Server to create a snapshot of the database which is then restored to the Remote Geographic Node server. On the active co-resident server all databases must be backed up.

Procedure

1. Log on to the Active Server.

2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
3. Click **Backup Locations**.
4. Click **Create**.
5. From the **Driver Letter** list, select the network drive on which you want to store the Contact Center Manager Server, CCT and ADMIN databases.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Backup Location. This location must be a shared folder with correct permissions.

   Important:

   If your contact center includes Contact Center Multimedia as a standalone server, do not use the same backup folder for your co-resident and multimedia ADMIN databases, as ADMIN databases stored in the same backup location overwrite each other.
7. In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the Windows password.
9. Click **OK**.
10. In the left pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Disk**.
12. In the **Applications** section, select **CCMS**, **CCT** and **ADMIN**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.

Restoring the database on the Remote Geographic Node server

Before you begin

- Know the location of the backup database.
- Stop all Contact Center services using the SCMU utility, if services are running.
- Ensure the patch level on the Remote Geographic Node server is the same as the Active Server.

Important:

Not all CCT data is stored in the database; therefore the following data must be configured on the Remote Geographic Node server, CCT License, CCT Contact Management Framework, CCT SOA configuration and CCT logging location. For information about CCT commissioning, see Communication Control Toolkit commissioning for Contact Center on page 219.

Important:

You must restore all databases in a co-resident server. Restoring only CCMS and not CCT or ADMIN may leave an inconsistent server and HA cannot shadow data correctly.

Important:

Restoring the Admin database can change configuration of Backup locations on the Remote Geographic Node server if the Active Server and Remote Geographic Node server backup locations are different. Therefore, after you restore the ADMIN database, close and reopen the Database and Maintenance utility.

Important:

The Server Configuration Tool must be run after a database restore has been performed and the administrator must check the data to ensure that it is correct.

About this task

Restore the database from the Active Server to the Remote Geographic Node server to ensure the databases are consistent. The Database Maintenance utility can restore only one application database at a time. Restore the data for the CCMS, CCT, and ADMIN databases

You must restore the CCMS, CCT, and ADMIN database onto the Remote Geographic Node server. You must restore the ADMIN database last.

Procedure

1. Log on to the Remote Geographic Node server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
3. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
4. In the right pane, under **Media Type**, select the media type on which the backup is restored.
5. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
6. Under **Application**, select the database to restore, either CCMS, CCT or ADMIN.
7. Under **Restore contents**, select **Data**.
8. Click **Restore**.
9. Use the **Progress information** field to monitor the progress of the restoration.

10. Repeat steps 6 to 8 to restore all databases.
11. Click **Exit** to close the Database Maintenance utility.

Variable definitions

Name	Description
Application	The database and applications of Contact Center that you can back up.
Backup Location	The destination of the network disk. The values are configured in the Backup Locations.
Restore contents	The type of content that is stored in the database. Data is in the database. Schema is the data for the database structure, tables and procedures.
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.

Configuring server details on the Remote Geographic Node server

Before you begin

- The Active Server databases are restored on to the Remote Geographic Node server.

About this task

After you restore the Active Server database on to the Remote Geographic Node server, the Remote Geographic Node server database contains the same agent and statistical data as the Active Server. However the Remote Geographic Node server details are now also configured exactly the same as the Active Server, therefore you must reconfigure the Remote Geographic Node server with its own server details.

Important:

Changes to the SIP Local Subscriber data may require a Contact Center Manager Server restart. Changes to the SIP Local Subscriber data may require updates to other Avaya Aura®

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

Procedure

1. Log on to the Remote Geographic Node server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
3. In the **Server Configuration** dialog box, click the **Local Settings** tab.
4. Update the Remote Geographic Node server local settings.
5. Click **Apply All**.
6. In the **Server Configuration** dialog box, click the **Licensing** tab.
7. Update the Remote Geographic Node server licensing details.
8. Click **Apply All**.
9. Click **OK**.
10. In the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.
11. Update the Remote Geographic Node server **SIP Network Settings** details.
12. Click **Apply All**.
13. Click **OK**.
14. In the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.
15. Update the Remote Geographic Node server **SIP Local Subscriber** details.
16. Click **Apply All**.
17. Click **OK**.
18. Click **Exit**.

Variable definitions

Name	Description
Avaya Server Subnet IP Address	The IP address of the subnet that connects the Contact Center servers (Contact Center Manager Server, Network Control Center, Contact Center Manager Administration, and Contact Center Multimedia).

Name	Description
Voice Proxy Server • IP or FQDN • Port • Network Transport	Information about the server that provides support for inbound and outbound calls, such as routing a call to an agent telephone. If the contact center uses an Avaya Aura® Session Manager, enter the IP address or Fully Qualified Domain Name (FQDN) for the primary Session Manager here. The server listening port. The default port is 5060. The SIP Network Transport communication protocol. Avaya recommends that you use TCP for Avaya Communication Server 1000.
CTI Proxy Server • IP or FQDN • Port • Network Transport • Port • Network Transport	Information about the server that provides support for SIP Computer Telephony Integration (CTI) so that Agent Desktop can acquire and control agent telephones for TR87. If the contact center uses an Avaya Aura® Application Enablement Services server, enter the IP address or Fully Qualified Domain Name (FQDN) for it here. For an Avaya Communication Server 1000 the default SIP CTI Proxy Server port is 5060. For an Application Enablement Services server the default SIP CTI Proxy Server port is 4723. The SIP Network Transport communication protocol. For an Application Enablement Services server, the default Network Transport communication protocol is TLS. The server listening port. The default port is 5060. The Backup Voice Proxy Server transport protocol.
IM Proxy Server • IP or FQDN • Port • Network Transport	Information about the server that supports the deployment of Instant Message over SIP. From the IM Provider list, select the name of the instant messaging provider. Select either Aura Presence Services or Microsoft OCS. The IP address or Fully Qualified Domain Name (FQDN) of the SIP IM Proxy Server. The default SIP IM Proxy Server port is 5222. The IM SIP Proxy Server transport protocol.

Name	Description
IM Provider	Select your IM Provider, Microsoft OCS or Aura Presence Services.
XMPP Domain	If using an Avaya Aura® Presence Services server, enter the domain name of the Extensible Messaging and Presence Protocol (XMPP) server.
Local SIP Subscriber • Contact Center Name • Domain Name • Password	Information about the environment of the SIP-enabled contact center and how to identify the server within the network. The registration user name on the registration proxy. Use a suitable user name following the standards in your system. Associated domain name for the SIP-enabled contact center. Password for the registration user name.
Web Service Ports	The Web Service Ports group box appears only if you select Avaya Aura® Presence Services as the IM Provider. Server Port default is 9100 Client Port default is 9120
SIP Server Type	Type of SIP proxy for the contact center integration. Depending on the switch type you select in the Application Selection window, the system automatically sets the specific SIP Server Type as the default. • For SIP Avaya Aura® 6.1 switch type, the default SIP Server Type is Avaya Aura® 6.1.
MS Locale	Locale (including language and dialects) of the system environment.
Local Listening Ports	The SIP Communication protocol accepted by the system for incoming calls. TCP/UDP Port default is 5060 TLS Port default is 5061

Configuring High Availability on the Remote Geographic Node server

Before you begin

- The Active Server databases are restored on to the Remote Geographic Node server.

About this task

Configure High Availability resiliency on the Remote Geographic Node server using the High Availability utility. The co-resident CCMS and CCT Remote Geographic Node Server shadows the Active Server.

Procedure

1. Log on to the Remote Geographic Node server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.
4. Double-click **Server Mode**.
5. Under **Server Mode**, select **Standby**.
6. Under **IP Configuration**, in the **Active CLAN** box, type the Managed IP address for the campus server pair.
7. Under **IP Configuration**, in the **Standby CLAN** box, type the IP address for the Remote Geographic Node server.
8. Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server.
9. Under **SMMC Port Configuration**,in the **Remote SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the remote (active) server.
10. Under **SMMC Port Configuration**,in the **Local SMMC Port** box, type the port number for System Management and Monitoring Component (SMMC) on the local (standby) server.
11. Ensure the **Managed IP** box is empty.
12. Ensure the **Remote Geographic Node (Optional)** box is empty.
13. Click **OK**.

Variable definitions

Name	Description
Active CLAN	Type the virtual Managed IP address that is used by the Active Server for campus resiliency. The Remote Geographic Node server monitors the Managed IP address of the campus site. If the Active server on the campus site fails, the Standby server assumes the managed IP address and continues processing. The Remote Geographic Node server monitors this campus Managed IP address and therefore continues shadowing.
Standby CLAN	The IP address for the Remote Geographic Node server.
Trusted IP	The IP address of a trusted server that is not likely to go down so that both Active and Standby servers have a server to ping regularly to verify the network connection. Avaya recommends that you use an IP address from your IT infrastructure as the Trusted IP address.
Local SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the local (standby) server. The default port number is 57012.
Remote SMMC Port	The Network Management port number for System Management and Monitoring Component (SMMC) on the remote (active) server. The port number entered here must match the port number set on the remote (active) server. The default port number is 57012.

Starting the Active Server

About this task

Start the Active Server using the System Management and Monitoring Component (SMMC) system tray. Starting the Active Server starts CCMS, CCT, and system processes.

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.
4. Under **Switchover And Network Timeout Configuration**, select **Enable Switchover**.
5. Click **OK**.
6. On the Windows taskbar of the active server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**.
7. To verify that the Contact Center services are running using the SCMU, select **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**. Check the CCMS and CCT services are running.

Starting shadowing on the Remote Geographic Node Server

About this task

Start shadowing on the Remote Geographic Node Server using the System Management and Monitoring Component (SMMC) system tray.

The Standby co-resident CCMS and CCT server shadows the Active CCMS and CCT server, maintaining a near real-time local copy of the CCMS, CCT, and Administration databases. The Remote Geographic Node server is therefore configured with the most recent data.

Important:

You must backup the Active server database, restore it onto the Standby server, and enable shadowing within 24 hours. If the difference in time between the Active and Standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the Active server database and restore it onto the Standby server before re-enabling shadowing. Ensure that the system clock time on the Active and Standby servers are synchronized.

Procedure

1. Log on to the Remote Geographic Node server.
2. On Windows taskbar of the standby server, right-click on the System Management and Monitoring Component (SMMC) system tray, and select **Start HA System**.

3. To verify that the Contact Center services are stopped using the SCMU, select **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**. Check the CCMS and CCT services are **Shut down**.

Verifying High Availability is running on the Active Server

About this task

Verify that the co-resident CCMS and CCT Remote Geographic Node server is shadowing the Active server using the High Availability Utility. The System dialog box of the High Availability utility displays system information about the Active and the Remote Geographic Node servers.

The dialog box displays the followings information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information
- License information
- Databases shadowed
- Time of last record shadowed
- Database namespaces
- Local and remote information on system status, switchover, shadowing and network
- CC Application install information
- Database space and journaling information
- Database processes information

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. In the left pane, expand **Configuration**.
4. Select **System**.
5. Select **Get System Configuration**.

The most recent system information appears.

Chapter 24: High Availability campus co-resident server commissioning

This section describes how to configure hot-standby and warm standby High Availability (HA) for a pair of co-resident Contact Center Manager Server (CCMS) and Communication Control Toolkit (CCT) servers in a campus with one of the following:

- Hot-standby AML-based contact center with an Avaya Communication Server 1000 PABX.
- Warm standby SIP-enabled contact center with an Avaya Communication Server 1000 PABX.
- Warm standby SIP-enabled contact center with an Avaya Aura® Communication Manager and an Avaya Aura® SIP Enablement Services (SES) server.

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

For information about configuring Mission Critical High Availability (HA) resiliency in a SIP-enabled contact center with an Avaya Aura® Session Manager, see Mission Critical High Availability campus co-resident server commissioning on page 305.

High Availability Campus server commissioning overview:

In a co-resident CCMS and CCT server configuration, one co-resident server is the active server and one is the standby server. The active CCMS and CCT server actively processes scripts and contacts and records statistics. The standby server shadows the active server. The standby server copies all configuration changes made on the active server and monitors the active server status. If the active server fails, the standby server, running in standby mode, recognizes the failure and starts processing contacts. The active and standby co-resident CCMS and CCT servers are part of the same Avaya Aura® Contact Center and they must be in the same subnet IP address range for campus High Availability resiliency to work.

The standby server must be configured the same as the active server. The standby and active servers must have the same patch level and the same hard disk drive partitions. Configuration changes made to the active CCMS and CCT server during normal operation are automatically copied to the standby server so that the standby server can take over processing from the active server when necessary.

In a High Availability campus co-resident AML-based solution, a CCT service failure does not initiate an automatic switchover; if a CCT service stops it is restarted. In a campus co-resident solution, only a CCMS service failure, hardware, network, or database failure can initiate a switchover but only in the following situations:

- The switchover check box on both servers is selected.
- The standby server is shadowing the active server.
- A valid license file containing standby server license information for CCMS and CCT exists to allow switchover.

In a High Availability campus AML-based solution with a pair of standalone CCT servers, an active CCT service failure, hardware, network, or database failure can initiate a switchover.

If the Contact Center Administrator uses the Windows Service Control Manager (SCM) to stop a monitored service on an Active server, a switchover occurs. If the Contact Center Administrator uses the System Control and Monitor Utility (SCMU) to stop a monitored service on an Active server, a switchover does not occur.

Remote Geographic Node:

The High Availability feature supports a Remote Geographic Node server. A Remote Geographic Node server is similar to a standby server but it is used only to shadow data from the active server—it has no other responsibility. The Remote Geographic Node does not automatically take over if the active system fails. If the standby server and active server are in the same building, then a Remote Geographic Node on a remote site provides additional data protection by maintaining a remote copy of the configuration and statistical information.

Managed IP Address:

A Managed IP address is a virtual IP address that is attached to a network adapter on the active server. Each High Availability application server is assigned a static IP address. After the active server in each replication pair is determined, the active server attaches a Managed IP address to the network interface. The managed IP address is only assigned to the active server and it is used by all other contact center applications and clients to connect to that application. The standby server assumes this same managed IP address if it takes over processing and becomes the active application. The active server stops using the Managed IP when it stops being the active server.

High Availability Utility:

Configure High Availability resiliency for CCMS and CCT using the High Availability Utility in the Database Utilities. The High Availability Utility is used to configure which server is the active and which is the standby server. The HA utility also configures the Managed IP of the active server.

The High Availability Utility on an Active Server has the following dialogs under the Configuration tab:

- Server Mode
    - Configure the IP address for the Active and Standby servers
    - Configure the IP address for Trusted servers
    - Configure the IP address for the Remote Geographic Node
    - Identify if the server is Active or Standby
    - Enable Automatic Switchover

- Configure the switchover time-out. This is the wait time if a network outage occurs before an automatic switchover occurs

- Notifications
  - Configure an e-mail server for e-mail notifications
  - Configure where and how often to send e-mail notifications
  - Configure the e-mail character set
- System
  - Display information on the system status
  - Verify that shadowing is running

The High Availability utility on an Active Server has the following dialogs under the Tasks tab:

- CC Applications
  - Start or stop the system
  - Enable or disable CC applications
  - Enable or disable switchover on the CC applications
  - Display system information
- CC Configuration
  - Monitor application service status
  - Define which application services are stopped or started
  - Configure how often a service restarts before switching over to the standby server
- System Control
  - Initiate a manual switchover for the Active Server
  - Initiate Standby Server shadowing

To commission CCMS, CCT and CCMA see the following sections in this document:

- Contact Center Manager Server commissioning, see Contact Center Manager Server commissioning on page 33.
- Contact Center Manager Administration commissioning, see Contact Center Manager Administration commissioning on page 121.
- Communication Control Toolkit commissioning, see Communication Control Toolkit commissioning for Contact Center. on page 219

Prerequisites

- The active and standby servers must meet the planning and engineering specifications. For more information, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Ensure unused Network Interface Cards (NICs) are disabled.
- If using an Avaya Communication Server 1000 Release 6.0 PABX, patch MPLR30010 must be applied to the PABX to support Avaya Aura® Contact Center High Availability functionality.
- CCMS is installed on the Active and Standby servers using the same drive specification on each server. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCT is installed on the Active and Standby servers using the same drive specification on each server. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCMA is installed on the Active and the Standby servers. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCMA replication is configured. CCMA AD-LDS replication is setup at install time. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCMS is configured on the Active Server. For more information, see Contact Center Manager Server commissioning on page 33.
- CCT is configured on the Active Server. For more information, see Communication Control Toolkit commissioning for Contact Center on page 219.
- CCMA is configured on the Active Server. For more information, see Contact Center Manager Administration commissioning on page 121.
- Ensure that the active Contact Center Manager Server is added as a CCMS type server in the primary CCMA - “Server Properties” page. For more information, see Adding the Contact Center Manager Server to Contact Center Manager Administration on page 149.
- Ensure that the active Communication Control Toolkit is added as a CCT type server in the primary CCMA - “Server Properties” page. For more information, see Adding the CCT Server in CCMA on page 216.
- License Manager is installed on the Active and the Standby Server. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- The Active and Standby Server have a valid standby server license file.

- Ensure the Communication Control Toolkit server is on a domain. This is to allow the CCT clients automatically re-connect after a switchover.
- Before you commission High Availability, use System Control and Monitoring Utility (SCMU) to shut down all CCMS and CCT services on both the active and standby servers.

High Availability Campus server commissioning procedures

About this task

This task flow shows the sequence of procedures to commission High Availability Campus servers.

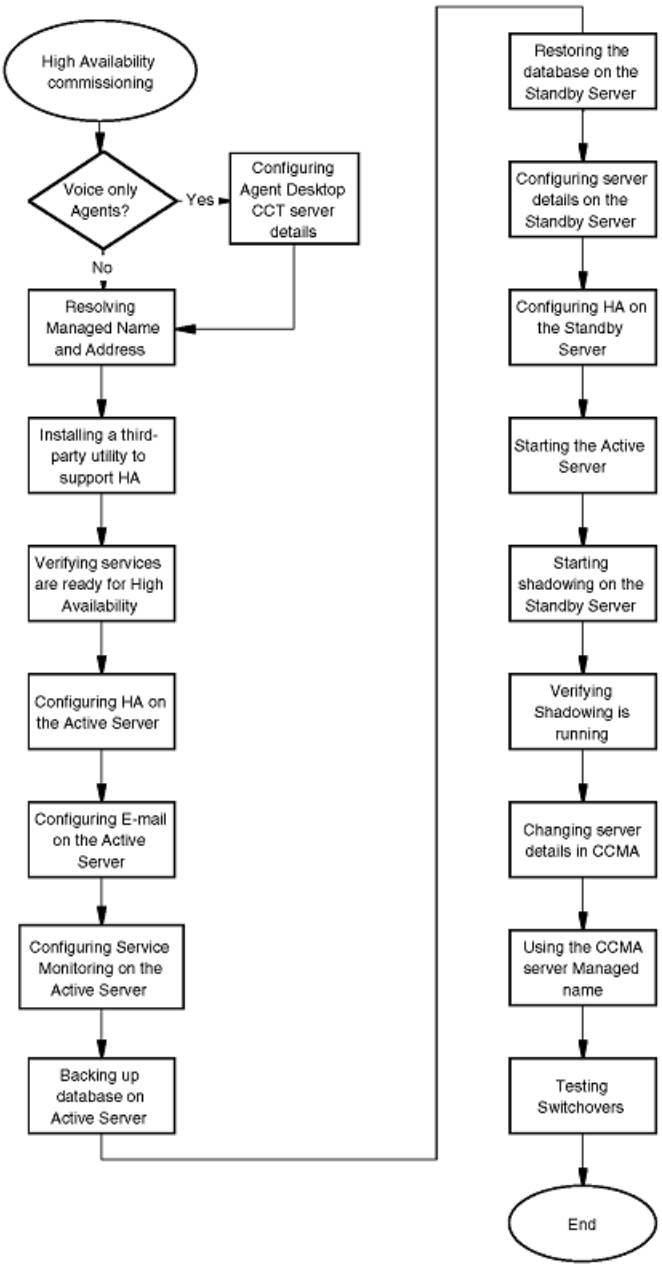


Figure 50: High Availability Campus server commissioning procedures

Configuring Agent Desktop CCT server details

About this task

In a voice-only campus High Availability solution use the Agent Desktop Telephony Toolbar configuration utility to configure Communication Control Toolkit (CCT) server.

In a multimedia-enabled solution Avaya Aura® Agent Desktop client software is typically downloaded from a Contact Center Multimedia (CCMM) server. Avaya Aura® Agent Desktop then communicates with that Contact Center Multimedia server to handle e-mail based contacts, and with a Communication Control Toolkit server to handle voice contacts.

In a multimedia-enabled High Availability solution use the CCMM Administration tool to configure standby CCMS and CCT server details. For more information about configuring standby CCMM and CCT server details, see Configuring CCMM General Administration on page 423.

A voice-only campus High Availability solution has two CCT servers, an Active CCT server and a Standby CCT server. The Managed IP address of the CCT High Availability pair is stored in a configuration file on the Active CCT server. Use the Agent Desktop Telephony Toolbar configuration utility to edit this file and configure the Agent Desktop CCT server details.

In a voice-only contact center the Avaya Aura® Agent Desktop client software is downloaded from the Agent Desktop Telephony Toolbar on the Active CCT server. Under normal operation Agent Desktop connects to the Active CCT server. If the Agent Desktop client software is unable to communicate with the Active CCT server, it re-connects using the Managed IP address and uses the Standby CCT server to handle voice contacts.

Procedure

1. Log on to the Active Communication Control Toolkit server.
2. Navigate to <Installed Drive>:\Avaya\Contact Center\Multimedia Server\Agent Desktop.
3. Double-click on **CCADConfigurator.exe** to start the Agent Desktop Toolbar configuration utility.
4. On the password message box, type the password. The default password is “ __avaya”.
5. Click **OK**.
6. On the **App Settings** tab, in the **CCTServer** row and in the **Value** column, type the Managed IP address of the CCT High Availability pair.
7. On the **App Settings** tab, in the **CCTBackupServer** row and in the **Value** column, ensure the name of the Standby CCT server is left blank.
8. Click **Save**.

9. Click **OK**.

Resolving the Managed name to the Managed IP Address

About this task

Complete the following procedure on the Active and Standby servers to resolve the Managed server name to the Managed IP address using the Windows hosts file. If the server has two network interfaces, apply these settings to the CLAN network interface. Each Contact Center server in a domain requires a DNS static entry.

Important:

Avaya Aura® Contact Center High Availability solutions do not support Windows Server 2008 Dynamic DNS.

Ask your System Administrator to add a Domain Name System (DNS) static entry for the Active and Standby servers and one additional DNS static entry for the each Managed name and associated Managed IP address.

A typical High Availability campus solution with a pair of co-resident servers requires 3 DNS static entries; one DNS static entry for the active server, one DNS static entry for the standby server, and one DNS static entry for the Managed name and associated IP address.

Perform this procedure on the Active and Standby servers.

Procedure

1. Open Windows Explorer.
2. Go to the folder C:\Windows\system32\drivers\etc.
3. Double-click on the **hosts** file, select **Open**, and select **Notepad**.
   The hosts file opens in Notepad.
4. Add the Managed IP address and the Managed server name to the hosts file.

   Important:

   The Managed Server name can be a full name or netbios server name.

Installing a third-party utility to support High Availability

About this task

Install a third-party utility required by the Avaya Aura® Contact Center High Availability feature.

Perform this procedure on the Active and Standby servers.

Procedure

1. Log on to the Active Server.
2. Using Windows Explorer, navigate to <installation drive>:\Avaya\Contact Center \Manager Server\CCSMMC\thirdparty\winpcap.
3. Double-click **WinPcap_4_1_2.exe**.
4. On the WinPcap installer dialog, click **Next**.
5. On the WinPcap installer **Setup Wizard** dialog, click **Next**.
6. On the WinPcap installer **License Agreement** dialog, click **I Agree**.
7. On the WinPcap installer **Installation options** dialog, click **Install**.
8. On the WinPcap installer dialog, click **Finish**.
9. Repeat this procedure on the Standby Server.

Verifying services are ready for High Availability

About this task

Verify that all CCMS and CCT services stop before you configure High Availability. This ensures that all PBX resources are available to the Active Server when it starts.

Perform this procedure on the Active and Standby servers.

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**.
3. On the **CCMS** tab, check that all services are stopped.
4. If any service is running, click **Stop CCMS**.

5. On the **CCT** tab, check that all services are stopped.
6. If any service is running, click **Stop CCT**.
7. Close the **System Control and Monitor Utility** window.
8. Repeat this procedure on the Standby server.

Configuring High Availability on the Active Server

About this task

Configure High Availability resiliency on the Active Server using the High Availability Utility. The Active Server is the co-resident CCMS and CCT server that normally processes calls.

Procedure

1. Select one co-resident CCMS and CCT server to be the active server and log on.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.
4. Double-click **Server Mode**.
5. Under **Server Mode Configuration**, select **Active**.
6. Under **Server Mode Configuration**, select the **Switchover** check box.
7. Under **Server Mode Configuration**, in the text box, type the maximum length of time the network connectivity tests can continue to fail consecutively before corrective action is considered.
8. Under **Server Mode Configuration**, from the drop down list, select the unit of time for the network connectivity tests.
9. Under **IP Configuration**, type the **Managed IP**, **CLAN** and **ELAN** IP addresses.
10. Under **IP Configuration**, type the **Active Server details**, **CLAN** and **ELAN** IP addresses.
11. Under **IP Configuration** type the **Standby Server details**, **CLAN** and **ELAN** IP addresses.
12. In the **Address** box, type the IP address of the **Trusted IP** server.
13. In the **Address** box, type the IP address of the optional **Remote Geographic Node**.
14. Click **OK**.
    A system message box appears. You must stop the system before you save any information.

15. Click **Yes** to stop the system.

Important:

Enter the ELAN IP information only if the system has an Embedded LAN (ELAN) subnet configured. Once you enter the ELAN IP information in the High Availability Utility, you cannot switch back to a single subnet system. In order to successfully achieve this, you must switch back to a single subnet system before High Availability is configured.

Variable definitions

Name	Description
Server Mode Configuration - Network Timeout	The High Availability—Network Timeout value sets the maximum length of time the network connectivity test can continue to fail before corrective action is considered. Avaya recommends that you set Network Timeout high enough to be tolerant of normal network latency, but low enough to be responsive if a failure occurs.
Managed IP	The virtual Managed IP (MIP) address that is used by the Active Server for High Availability. The Active Server is always 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 occurred because the IP address does not change. A MIP is used only 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 Address	The Active and Standby servers use the Trusted IP address to verify network connectivity. If the Active server cannot communicate with the Standby server it attempts to communicate with the Trusted IP address. If the Active Server cannot connect to the Trusted IP address on startup then no Contact Center services start on that server.

Name	Description
	If the Active server cannot communicate with the Trusted IP address, if shadowing and switchover are enabled, then the Active server stops processing contacts and shuts down. The Standby server starts processing contacts if it cannot communicate with the Active server but can communicate with the Trusted IP address. Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
Remote Geographic Node	The IP address of the optional Remote Geographic Node.

Procedure job aid

Configure High Availability on the active co-resident server.

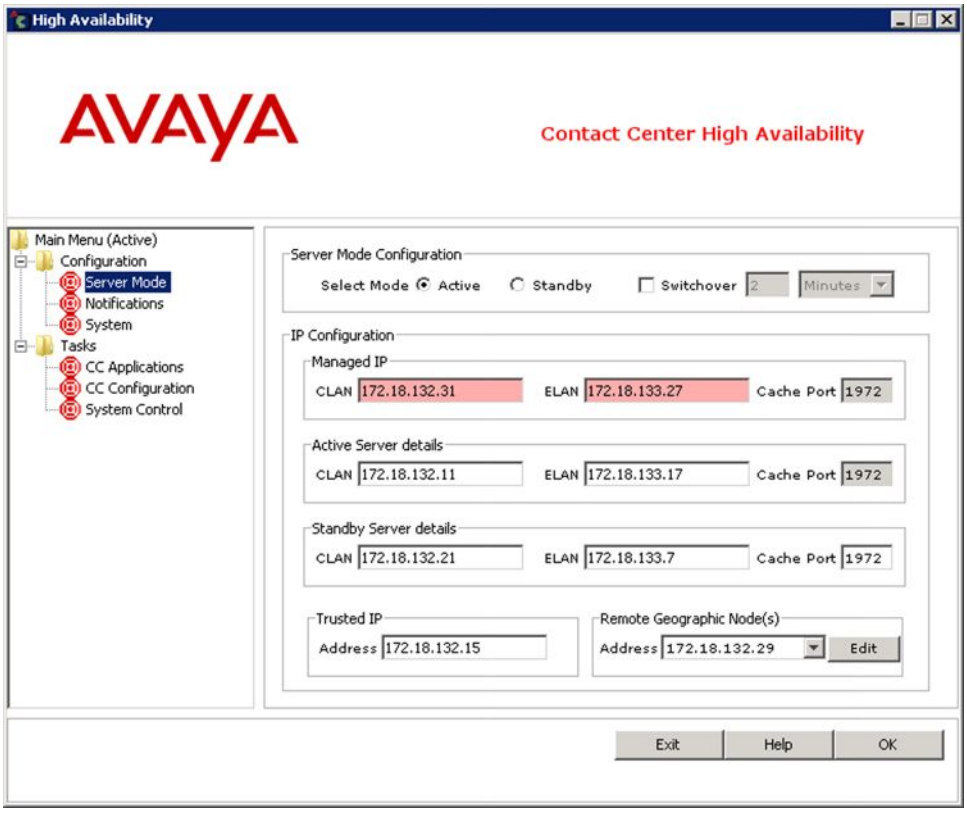


Figure 51: Example of configuring High Availability on the active server

Configuring E-mail notification on the Active Server

Before you begin

- If anonymous users are allowed, a user name and password may not be required. Check with the Administrator of the e-mail server for setup configuration.

About this task

If an automatic switchover occurs, the High Availability utility can send e-mail messages to configured users at a defined interval.

The default e-mail notification character set is US_ASCII. The following character sets are also supported:

- ISO-8859-1
- UTF-8
- UTF-16BE
- UTF-16LE
- UTF-16

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.
4. Double-click **Notification**.
5. Select the **Email** check box.
6. Type the **SMTP Server** name.
7. Type the **Username**.
8. Type the **Password**.
9. Type the **From Address**.
10. Type the **To Address** or **Addresses**.
11. Click **OK** to save the data.

Variable definitions

Name	Description
Email	Enables or disables e-mail notifications.
SMTP Server	The SMTP Server name, which is automatically verified when saving the data.
Username	E-mail User log on name.
Password	E-mail User log on 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.

Configuring service monitoring on the Active Server

About this task

The High Availability feature monitors a number of critical services on the Active Server. If these critical services stop or fail, they automatically restart in the correct order. If a critical service fails a defined number of times, the Active Server may, if Switchover is enabled, shut down and hand over processing to the Standby Server.

Critical services are listed, monitored, restarted, and controlled using the Contact Center Configuration tab on the Tasks tab of the High Availability utility. The Contact Center Configuration tab lists the critical CCMS services and all of the CCT services on the co-resident 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 occurs.

For switchover to occur, both the Active and the Standby servers must have their respective switchover check box 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 RestartThreshold is the time period within when the services are monitored and the counters are increased when services fail. When this threshold is met, the counters are reset to zero, monitoring restarts, and the restart threshold timer resets.

Procedure

1. Log on to the Active Server.
2. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. In the **High Availability** window, in the left pane, expand the **Tasks** folder.
4. Double-click **CC Configuration**.
5. For each service to monitor, select the **Monitor** check box.
6. For each service to restart, select the **Restart** check box.

   Important:

   By default service monitoring is selected for CCT and is not selected for CCMS.
7. In the **Start Wait Time** column, type the number of seconds to wait before restarting a service.
8. For CCT only, in the **Stop Wait Time** column, type the number of seconds to wait before stopping a service.
9. In the **Restart Limit** column, type the maximum number of attempts to restart the service before switchover occurs.This Administrator decides the maximum number.
10. In the **Restart Threshold** column, type the time in seconds to reset the restart counter (for each service that is restarted) after the threshold is passed.

Variable definitions

Name	Description
CC	The Contact Center application name, CCMS or CCT in this case, because CCMS and CCT are co-resident.
Service	The application service name, for example OAM_Service.
Monitor	Used to enable or disable the service monitoring.
Restart	Restart the service if it stops.
Start Wait Timer	The time in seconds that service monitor waits before attempting to restart or initiating

Name	Description
	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. For example, if service monitor stopped this service, service monitor checks the status if the status is not SERVICE_STOPPED, it waits for Stop Wait Time before attempting to start the service.
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.

Procedure job aid

This section provides an example of the service monitor configuration in the High Availability Utility.

When the CCMS OAM service has stopped 3 times for longer than 60 seconds in a period of 12 hours, initiate an automatic switchover. This requirement is achieved by setting the OAM service configuration values to the following settings:

CC	CCMS
Service	OAM_Service
Monitor	Selected
Restart	Selected
Start Wait Timer	60 Seconds
Restart Limit	3
Restart Threshold	43200 Seconds (12 hours)

Backing up the database on the Active Server

About this task

The Active Server is configured for High Availability. Now the Standby Server must be prepared for High Availability resiliency. Back up the Active Server to create a snapshot of the database which is then restored to the Standby Server. On the active co-resident server all databases must be backed-up.

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
3. Click **Backup Locations**.
4. Click **Create**.
5. From the **Driver Letter** list, select the network drive on which you want to store the Contact Center Manager Server, CCT and ADMIN databases.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Backup Location. This location must be a shared folder with correct permissions.

   Important:

   If your contact center includes Contact Center Multimedia as a standalone server, do not use the same backup folder for your co-resident and multimedia ADMIN databases, as ADMIN databases stored in the same backup location overwrite each other.
7. In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the Windows password.
9. Click **OK**.
10. In the left pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Disk**.
12. In the **Applications** section, select **CCMS**, **CCT** and **ADMIN**.
13. From the **Backup Location** list, select the network drive on which to store the backup.

14. Click **Backup**.

Restoring the database on the Standby Server

Before you begin

- Know the location of the backup database.
- Ensure no traffic is running on the Standby Server.
- Stop shadowing if shadowing is running on the Standby Server.
- Stop all Contact Center services using the SCMU utility, if services are running.
- Ensure the patch level on the Standby Server is the same as the Active Server.

Important:

Not all CCT data is stored in the database; therefore the following data must be configured on the Standby Server, the CCT Communication Server 1000 service provider, CCT License, CCT Contact Management Framework, CCT SOA configuration and CCT logging location. For information about CCT commissioning, see Communication Control Toolkit commissioning for Contact Center on page 219.

Important:

You must restore all databases in a co-resident server. Restoring only CCMS and not CCT or ADMIN may leave an inconsistent server and HA cannot shadow data correctly.

Important:

Restoring the Admin database can change configuration of Backup locations on the Standby Server if the Active Server and Standby Server backup locations are different. Therefore, after you restore the ADMIN database, close and reopen the Database and Maintenance utility.

Important:

Run the Server Configuration utility after performing a database restore and check that the data is correct.

About this task

Restore the database from the Active Server to the Standby Server to ensure the databases are consistent. The Database Maintenance utility can restore only one application database at a time. Restore the data for the CCMS, CCT, and ADMIN databases

You must restore the CCMS, CCT, and ADMIN database onto the Standby Server. You must restore the ADMIN database last.

Procedure

1. Log on to the Standby Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
3. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
4. In the right pane, under **Media Type**, select the media type on which the backup is restored.
5. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
6. Under **Application**, select the database to restore, either CCMS, CCT or ADMIN.
7. Under **Restore contents**, select Data.
8. Click **Restore**.
9. Use the **Progress information** field to monitor the progress of the restoration.
10. Repeat steps 6 to 8 to restore all databases.
11. Click **Exit** to close the Database Maintenance utility.

Variable definitions

Name	Description
Application	The database and applications of Contact Center that you can back up.
Backup Location	The destination of the network disk. The values are configured in the Backup Locations.
Restore contents	The type of content that is stored in the database. Data is in the database. Schema is the data for the database structure, tables and procedures.
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.

Configuring server details on the Standby Server

Before you begin

- The Active Server databases are restored on to the Standby Server.

About this task

After you restore the Active Server database on to the Standby Server, the Standby Server database contains the same agent and statistical data as the Active Server. However the Standby Server server details are now also configured exactly the same as the Active Server, therefore you must reconfigure the Standby Server with its own server details.

Important:

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

Procedure

1. Log on to the Standby Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
3. In the **Server Configuration** dialog box, click the **Local Settings** tab.
4. Update the Standby Server local settings.
5. Click **Apply All**.
6. In the **Server Configuration** dialog box, click the **Licensing** tab.
7. Update the Standby Server licensing details.
8. Click **Apply All**.
9. Click **OK**.
10. If your contact center is AML-based, in the **Server Configuration** dialog box, click the **Switch CS 1000** tab.
11. Update the Avaya Communication Server 1000 PABX Data details.
12. Click **Apply All**.
13. Click **OK**.
14. If your contact center is SIP-enabled, in the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.
15. Update the Standby Server **SIP Network Settings** details.

16. Click **Apply All**.
17. Click **OK**.
18. If your contact center is SIP-enabled, in the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.
19. Update the Standby Server **SIP Local Subscriber** details.
20. Click **Apply All**.
21. Click **OK**.
22. Click **Exit**.

Variable definitions

Name	Description
Avaya Server Subnet IP Address	The IP address of the subnet that connects the Contact Center servers (Contact Center Manager Server, Network Control Center, Contact Center Manager Administration, and Contact Center Multimedia are connected.
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

Name	Description
	working with an Avaya Communication Server 1000 PABX.
CallPilot Port	The port number of the primary Avaya CallPilot® voice connection type to the Contact Center Manager Server when working with an Avaya Communication Server 1000 PABX. The default port is 5060.
PABX Customer Number	The customer number for the PABX.
PABX IP Address	The IP address of the PABX.
PABX Name	The name of the Avaya Communication Server 1000 PABX. Valid characters for PABX names are A-Z, a-z, 0-9, underscore (_), and period (.). PABX names must begin with an alphabetical character and cannot contain spaces. The last character must not be an underscore or period. PABX names must not exceed 80 characters in length.
Voice Proxy Server • IP or FQDN • Port • Network Transport	Information about the server that provides support for inbound and outbound calls, such as routing a call to an agent telephone. If the contact center uses an Avaya Communication Server 1000 Network Routing Service (NRS), enter the IP address or Fully Qualified Domain Name (FQDN) for it here. If the contact center uses an Avaya Aura® Session Manager, enter the IP address or Fully Qualified Domain Name (FQDN) for the primary Session Manager here. If the contact center uses an Avaya Aura® SIP Enablement Services (SES) server, enter the IP address or Fully Qualified Domain Name (FQDN) for it here. The server listening port. The default port is 5060. The SIP Network Transport communication protocol. Avaya recommends that you use TCP for Avaya Communication Server 1000.

Comments? infodev@avaya.com

Name	Description
CTI Proxy Server • IP or FQDN • Port • Network Transport	Information about the server that provides support for SIP Computer Telephony Integration (CTI) so that Agent Desktop can acquire and control agent telephones for TR87. If the contact center uses an Avaya Communication Server 1000 Signaling Server, enter the IP address or Fully Qualified Domain Name (FQDN) for it here. If the contact center uses an Avaya Aura® Application Enablement Services server, enter the IP address or Fully Qualified Domain Name (FQDN) for it here. For an Avaya Communication Server 1000 the default SIP CTI Proxy Server port is 5060. For an Application Enablement Services server the default SIP CTI Proxy Server port is 4723. The SIP Network Transport communication protocol. For an Avaya Communication Server 1000, the default Network Transport communication protocol is TCP. For an Application Enablement Services server, the default Network Transport communication protocol is TLS.
Backup Voice Proxy Server • IP or FQDN • Port • Network Transport	Information about the server that provides backup support for inbound and outbound calls, such as routing a call to an agent telephone. Avaya Aura® Contact Center must have a Standby Server license to support a Backup Voice Proxy Server. The only type of Backup Voice Proxy Server supported by Avaya Aura® Contact Center is an Avaya Aura® Session Manager when it used with an Avaya Aura® Communication Manager. If the contact center uses an Avaya Aura® Communication Manager and a backup Avaya Aura® Session Manager, enter the IP address or Fully Qualified Domain Name (FQDN) for the backup Session Manager here. The server listening port. The default port is 5060. The Backup Voice Proxy Server transport protocol.

Name	Description
IM Proxy Server • IP or FQDN • Port • Network Transport	Information about the server that supports the deployment of Instant Message over SIP. From the IM Provider list, select the name of the instant messaging provider. Select either Avaya Aura® Presence Services or Microsoft OCS. The IP address or Fully Qualified Domain Name (FQDN) of the SIP IM Proxy Server. The default SIP IM Proxy Server port is 5222. The IM SIP Proxy Server transport protocol.
IM Provider	Select your IM Provider, Microsoft OCS or Avaya Aura® Presence Services.
XMPP Domain	If using an Avaya Aura® Presence Services server, enter the domain name of the Extensible Messaging and Presence Protocol (XMPP) server.
Local SIP Subscriber • Contact Center Name • Domain Name • Password	Information about the environment of the SIP-enabled contact center and how to identify the server within the network. The registration user name on the registration proxy. Use a suitable user name following the standards in your system. Associated domain name for the SIP-enabled contact center. Password for the registration user name.
Web Service Ports	The Web Service Ports group box appears only if you select Avaya Aura® Presence Services as the IM Provider. Server Port default is 9100 Client Port default is 9120
SIP Server Type	Type of SIP proxy for the contact center integration. Depending on the switch type you select in the Application Selection window, the system automatically sets the specific SIP Server Type as the default. • For SIP Avaya Aura® 6.1 switch type, the default SIP Server Type is Avaya Aura® 6.1. • For SIP Avaya Communication Server 1000 switch type, the default SIP Server Type is CS1000.

Name	Description
MS Locale	Locale (including language and dialects) of the system environment.
Local Listening Ports	The SIP Communication protocol accepted by the system for incoming calls. TCP/UDP Port default is 5060 TLS Port default is 5061

Configuring High Availability on the Standby Server

Before you begin

- The Active Server databases are restored on to the Standby Server.

About this task

Configure High Availability resiliency on the Standby Server using the High Availability utility. The co-resident CCMS and CCT Standby Server shadows the Active Server and takes over processing if the Active Server fails.

Procedure

1. Log on to the Standby Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. In the left pane of the **High Availability** dialog box, click **Server Mode**.
4. In the **Server Mode Configuration** section, select **Standby**.
5. Under **Server Mode Configuration**, in the text box, type the maximum length of time the network connectivity tests can continue to fail consecutively before corrective action is considered.
6. Under **Server Mode Configuration**, from the drop down list, select the unit of time for the network connectivity tests.
7. Under **IP Configuration**, type the **Active Server details**, **CLAN** and **ELAN** IP addresses.
8. Under **IP Configuration**, type the **Standby Server details**, **CLAN** and **ELAN** IP addresses.
9. Under **IP Configuration**, in the **Trusted IP** box, type the IP address of a trusted server.
10. Click **OK**.
    A system message box appears. You must stop the system before you save any information.

11. Click **OK**.

Variable definitions

Name	Description
Managed IP	The virtual Managed IP (MIP) address that is used for both the Active and Standby servers for campus resiliency. The Active Server is always 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 occurred because the IP address does not change. A MIP is used only 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 Active and Standby servers use the Trusted IP address to verify network connectivity. If the Active server cannot communicate with the Standby server it attempts to communicate with the Trusted IP address. If the Active Server cannot connect to the Trusted IP address on startup then no Contact Center services start on that server. If the Active server cannot communicate with the Trusted IP address, if shadowing and switchover are enabled, then the Active server stops processing contacts and shuts down. The Standby server starts processing contacts if it cannot communicate with the Active server but can communicate with the Trusted IP address. Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to ping request, as the Trusted IP address.

Procedure job aid

Configure High Availability on the standby co-resident server.

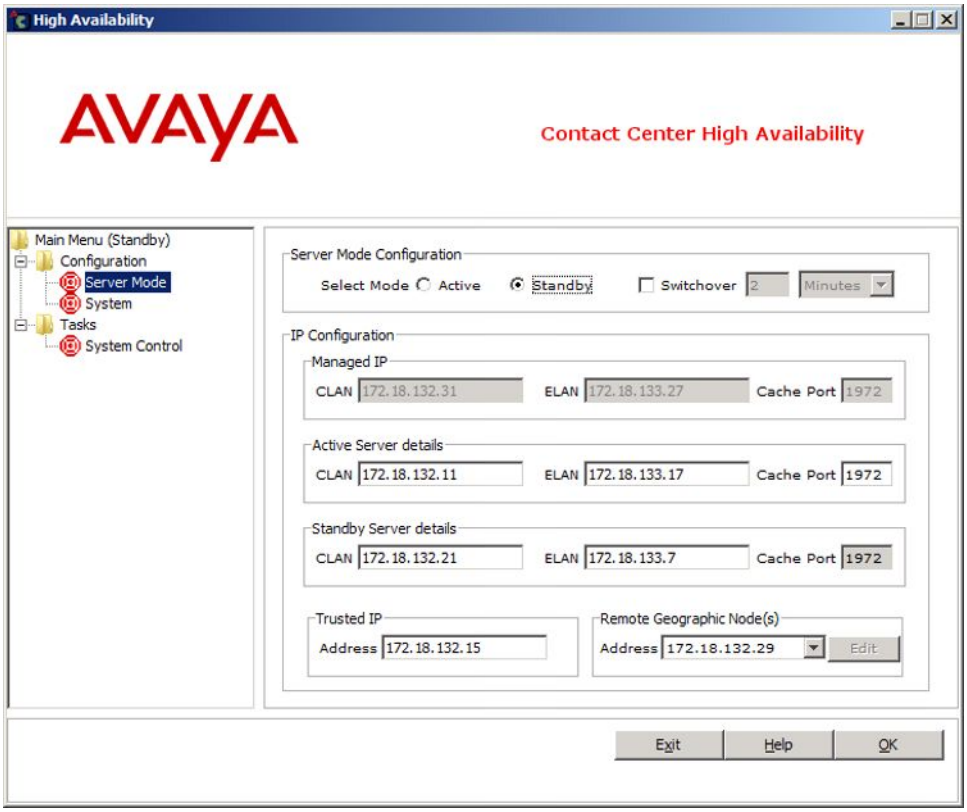


Figure 52: Example of configuring High Availability on the standby server

Starting the Active Server

About this task

Start the Active Server using the High Availability utility. Starting the Active Server starts CCMS, CCT, and system processes.

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Tasks**.

4. Double-click **CC Applications**.
5. In the first box under **CC Applications**, select the system.
6. Click **Start**.
   A delay occurs before all Contact Center services start.
7. Click **OK**.
8. To verify that the Contact Center services are running using the SCMU, select **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**. Check the CCMS and CCT services are running.

Procedure job aid

After the system starts, check that the Managed IP (MIP) address is assigned to the network adapter of the Active Server by opening a command window and entering:

```
IPCONFIG /all
```

The IP and the MIP of the Active Server appears.

Starting shadowing on the Standby Server

Before you begin

Important:

Enabling the shadowing functionality is available only on the system control dialog box of the High Availability utility on the Standby Server.

Important:

It is advisable on the Standby Server not to stop and start shadowing but to use the pause and resume functionality.

About this task

Start shadowing on the Standby Server using the High Availability utility. The Standby co-resident CCMS and CCT server must be shadowing the Active CCMS and CCT server for switchover to occur if the Active Server fails. While the Standby server is shadowing the Active server, it maintains a near real-time local copy of the CCMS, CCT, and Administration databases. Therefore, the Standby Server is configured with the most recent data and it can take over from the Active Server if necessary.

Important:

You must backup the Active server database, restore it onto the Standby server, and enable shadowing within 24 hours. If the difference in time between the Active and Standby server

database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the Active server database and restore it onto the Standby server before re-enabling shadowing. Ensure that the system clock time on the Active and Standby servers are synchronized.

Procedure

1. Log on to the Standby Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Tasks**.
4. Double-click **System Control**.
5. In the **Control** box, select **Shadowing**.
6. Click **Start**.
7. Click **OK**.
8. To verify that the CCMS services are stopped using the SCMU, select **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**. Check the CCMS services are stopped.
9. To verify that the CCT services are running using the SCMU, select **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**. Check the CCT services are running.

Procedure job aid

Example of starting shadowing on the standby server.

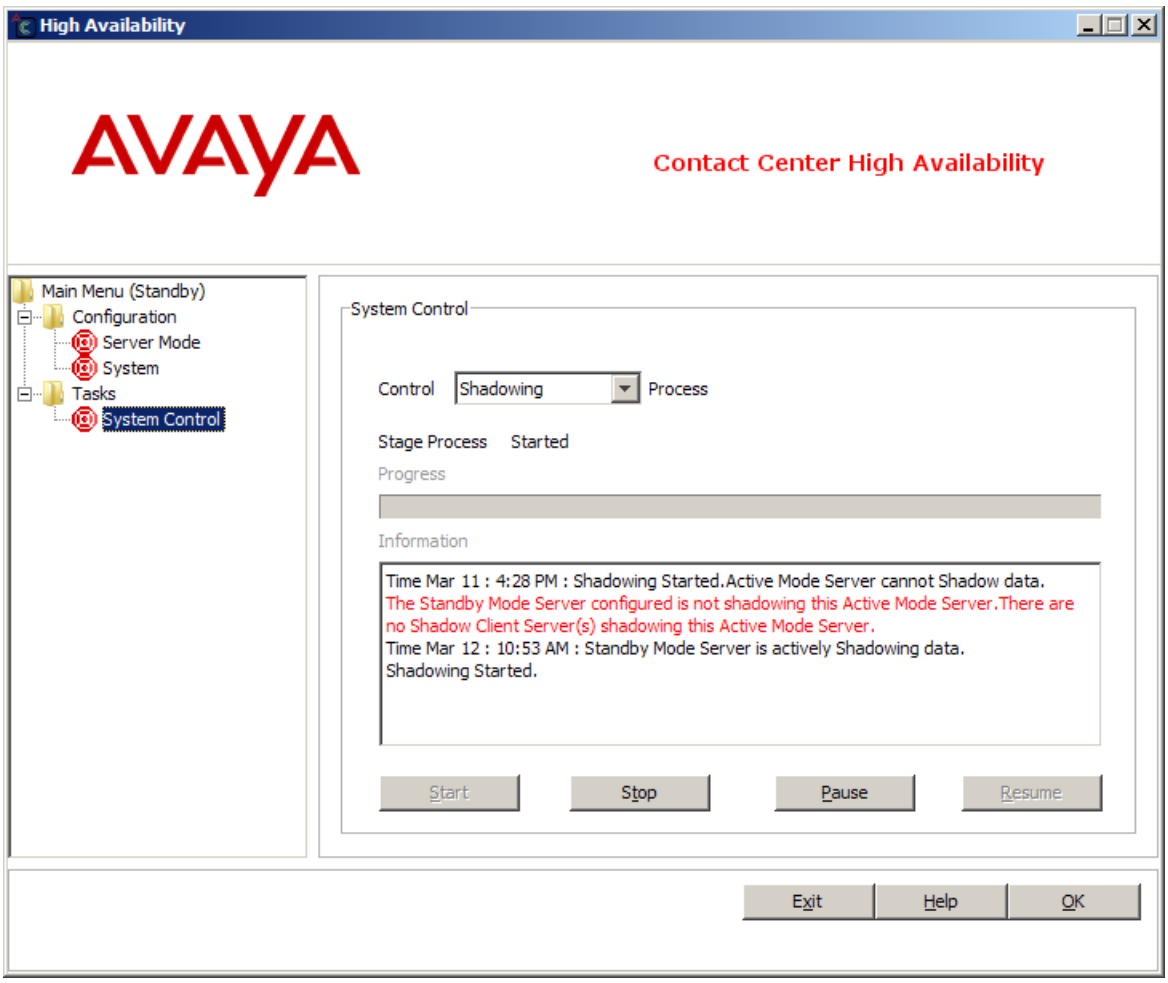


Figure 53: Starting shadowing on the Standby Server.

Verifying shadowing is running on the Active Server

About this task

Verify that the Standby co-resident CCMS and CCT server is shadowing the Active server using the High Availability Utility. The System dialog box of the High Availability utility displays system information about the Active and the Standby servers.

The dialog box displays the followings information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information

- Remote server connection status
- Remote server port information
- License information
- Databases shadowed
- Time of last record shadowed
- Database namespaces
- Local and remote information on system status, switchover, shadowing and network.
- CC Application install information
- Database space and journaling information
- Database processes information

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. In the left pane, expand **Configuration**.
4. Select **System**.
5. Select **Get System Configuration**.
   The most recent system information appears.

Procedure job aid

To verify that the Standby Server is shadowing the Active server, examine the Shadowing section of the System Configuration log on the Active server.

For example, look for the following text:

- Shadowing :
- Number of clients connected : 1
- List of Shadow Clients connected :
- AA.BB.CC.DD [port Number] Latency : 0 second Shadowing Rate :
- Last record of Shadowing was @ date and times shadowing started.

Where AA.BB.CC.DD is the IP address of the Standby server.

Changing server details in Contact Center Manager Administration

About this task

In Contact Center Manager Administration, change the Contact Center Manager Server and Communication Control Toolkit server details to use the High Availability Managed IP address and Managed name details.

The High Availability Managed IP address and Managed name details entered here must match those configured in Resolving the Managed name to the Managed IP Address on page 368.

Procedure

1. Log on to the active server.
2. Log on to the Contact Center Manager Administration application with administrative privileges.
3. On the **Launchpad**, click **Configuration**.
4. From the list of servers in the system tree, right-click on the active CCMS server, and select **Edit Properties**.
5. In the **Server Name** box, type the High Availability Managed name of the Contact Center Manager Server.
6. In the **IP Address** box, type the High Availability Managed IP address of the Contact Center Manager Server.
7. In the **Display Name** box, type the name of the Contact Center Manager Server as you want it to appear in the system tree of Contact Center Manager Administration.
8. Click **Submit**.
9. From the list of servers in the system tree, right-click on the active CCT server, and select **Edit Properties**.
10. In the **Server Name** box, type the High Availability Managed name of the Communication Control Toolkit server.
11. In the **IP Address** box, type the High Availability Managed IP address of the Communication Control Toolkit server.
12. In the **Display Name** box, type the name of the Communication Control Toolkit as you want it to appear in the system tree of Contact Center Manager Administration.

13. Click **Submit**.

Using the Contact Center Manager Administration server Managed name

Before you begin

- Configure High Availability on the Active and Standby servers.
- Change the server details in CCMA. For more information about changing the server details in CCMA, see Changing server details in Contact Center Manager Administration on page 392.
- Know the user ID and password to log on to the CCMA.

About this task

Use the High Availability Managed name of the Contact Center Manager Administration server access the CCMA application. When the Avaya Aura® Contact Center High Availability feature is configured and enabled, re-direct all Contact Center Manager Administration client Web browsers to use the Managed server name of the CCMA server.

If you have a High Availability campus co-resident solution Avaya recommends that you log on to the CCMA Web client using the Managed name of the co-resident CCMS and CCMA server. If an active application or server fails, the CCMA client Web browser continues to use the Managed name and you can continue working without interruption.

Important:

Do not type the real or Managed IP address in the Address box. Using an IP address results in problems with Scripting, Historical Reporting, Configuration, Contact Center Management, and Access and Partition Management.

Procedure

1. Start Internet Explorer.
2. In the **Address** box, type the URL of the CCMA server. The default URL is http://<server name>; where <server name> is the Managed server name of the CCMA server.
3. In the **User ID** box, type your user ID.
4. In the **Password** box, type your password.
5. Click **Login**.

Testing switchovers

Before you begin

- Configure High Availability on the Active and Standby servers.

About this task

Test the High Availability feature and infrastructure by making a manual switchover from the Active server to the Standby server.

Procedure

1. Log on to the current Active 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. Under **Tasks**, double-click **System Control**.
5. In the **Control** box, select **Switchover**.
6. Select the **System** tab.
7. Select **Switchover**.
8. Click **Start**.

Procedure job aid

When the Standby Server becomes the new Active Server, test the Standby Server configuration by making a call using the CCT Reference Client. For more details, see Verifying CCT using the Reference Client on page 235.

Chapter 25: High Availability Geographic co-resident server commissioning

This section describes how to configure geographic High Availability (HA) in an Avaya Communication Server 1000 based solution. Avaya Aura® Contact Center geographic High Availability supports data resiliency and Disaster Recovery.

Avaya Aura® Contact Center supports hot-standby and warm standby geographic High Availability for the following solutions:

- Hot-standby AML-based contact center with an Avaya Communication Server 1000 Release 6.0 or later PABX.
- Warm standby SIP-enabled contact center with an Avaya Communication Server 1000 Release 6.0 or later PABX.

For information about configuring geographic High Availability resiliency for a pair of co-resident CCMS and CCT servers in an Avaya Aura® platform Release 6.1 or Release 6.2 based solution, see High Availability Remote Geographic Node server commissioning on page 337.

In geographic Wide Area Network solutions the standby server on the remote geographic site is called a Remote Geographic Node server. The Active server and the Remote Geographic Node server are part of the same Avaya Aura® Contact Center solution but they are typically in different geographic locations and subnets.

The Active server may also have a local Standby server in the same campus location. The Standby server shadows the Active server. If the Active server fails the local Standby server takes over call processing on the local site.

The Remote Geographic Node server on the remote site shadows the Active server on the campus site. If the Active server fails, the local Standby server assumes the shared Managed IP address and starts processing calls. The Remote Geographic Node server monitors the campus Managed IP address so it continues shadowing.

Remote Geographic Node server commissioning overview:

In a geographic co-resident CCMS and CCT server configuration, one server is the Active server and one is the Remote Geographic Node server. The active CCMS and CCT server actively processes scripts and contacts and records statistics. The Remote Geographic Node server shadows the active server. The Remote Geographic Node server copies all configuration changes made on the Active server and monitors the Active server status. The Remote Geographic Node server does not automatically take over if the active system fails. You must start the Remote Geographic Node server manually.

The Remote Geographic Node server must be configured the same as the active server. The Remote Geographic Node and active servers must have the same patch level and the same hard disk drive partitions. Configuration changes made to the active CCMS and CCT server during normal operation are automatically copied to the Remote Geographic Node server by the shadowing process.

High Availability Utility:

Configure High Availability resiliency for CCMS and CCT using the High Availability Utility in the Database Utilities. The High Availability Utility is used to configure which server is the active and which is Remote Geographic Node server.

The High Availability Utility on an Active Server has the following dialogs under the Configuration tab:

- Server Mode
  - Configure the IP address for the Active and Remote Geographic Node servers
  - Configure the IP address for Trusted servers
  - Configure the IP address for a Remote Geographic Node
  - Identify if the server is Active or a Remote Geographic Node (Server Mode - Standby)
  - Enable Automatic Switchover
  - Configure the switchover time-out. This is the wait time if a network outage occurs before an automatic switchover occurs
- Notifications
  - Configure an e-mail server for e-mail notifications
  - Configure where and how often to send e-mail notifications
  - Configure the e-mail character set
- System
  - Display information on the system status
  - Verify that shadowing is running

The High Availability utility on an Active Server has the following dialogs under the Tasks tab:

- CC Applications
  - Start or stop the system
  - Enable or disable CC applications
  - Enable or disable switchover on the CC applications
  - Display system information
- CC Configuration
  - Monitor application service status
  - Define which application services are stopped or started

  - Configure how often a service restarts before switching over to the Remote Geographic Node server

- System Control
  - Initiate a manual switchover for the Active Server
  - Initiate Remote Geographic Node server shadowing

To commission CCMS, CCT and CCMA see the following sections in this document:

- Contact Center Manager Server commissioning, see Contact Center Manager Server commissioning on page 33
- Contact Center Manager Administration commissioning, see Contact Center Manager Administration commissioning on page 121
- Communication Control Toolkit commissioning, see Communication Control Toolkit commissioning for Contact Center on page 219

Prerequisites

- The active and Remote Geographic Node servers must meet the planning and engineering specifications. For more information, see *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Ensure unused Network Interface Cards (NICs) are disabled.
- CCMS is installed on the Active and Remote Geographic Node servers using the same drive specification on each server. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCT is installed on the Active and Remote Geographic Node servers using the same drive specification on each server. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCMA is installed on the Active and the Remote Geographic Node servers. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCMA replication is configured. CCMA Replication is setup at install time. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCMS is configured on the Active Server. For more information, see Contact Center Manager Server commissioning on page 33.
- CCT is configured on the Active Server. For more information, see Communication Control Toolkit commissioning for Contact Center on page 219.
- CCMA is configured on the Active Server. For more information, see Contact Center Manager Administration commissioning on page 121.

- License Manager is installed on the Active and the Remote Geographic Node server. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- Have a valid Remote Geographic Node server license file on the Active and Remote Geographic Node server.
- Ensure the Communication Control Toolkit server is on a domain. This is to allow the CCT clients to automatically re-connect after a switchover.
- Before you commission High Availability, use System Control and Monitoring Utility (SCMU) to shut down all CCMS and CCT services on both the active and Remote Geographic Node servers.

High Availability Geographic co-resident server commissioning procedures

About this task

This task flow shows the sequence of procedures to commission High Availability Geographic servers.

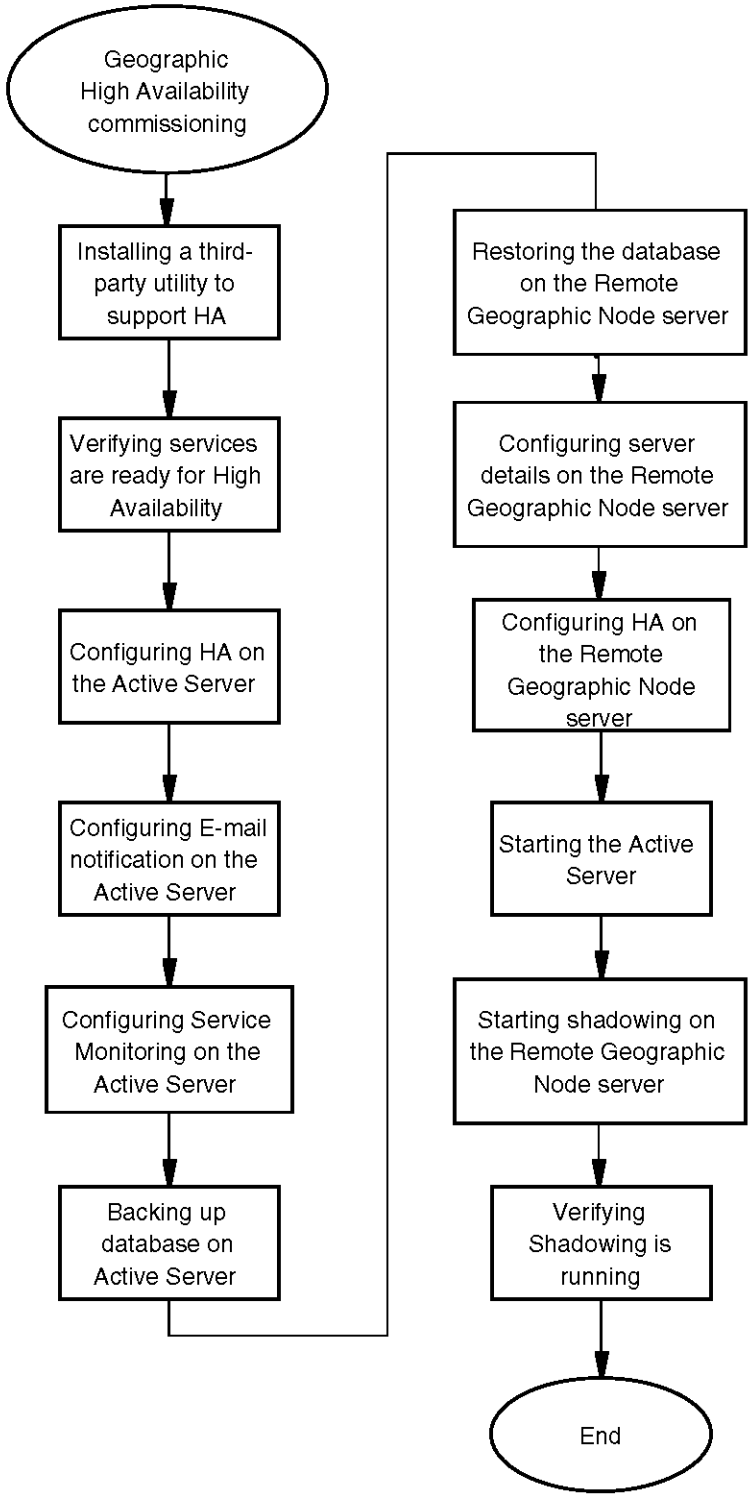


Figure 54: High Availability Geographic co-resident server commissioning procedures

Installing a third-party utility to support High Availability

About this task

Install a third-party utility required by the Avaya Aura® Contact Center High Availability feature.

Perform this procedure on the Active and Remote Geographic Node servers.

Procedure

1. Log on to the Active Server.
2. Using Windows Explorer, navigate to <installation drive>:\Avaya\Contact Center \Manager Server\CCSMMC\thirdparty\winpcap.
3. Double-click **WinPcap_4_1_2.exe**.
4. On the WinPcap installer dialog, click **Next**.
5. On the WinPcap installer **Setup Wizard** dialog box, click **Next**.
6. On the WinPcap installer **License Agreement** dialog box, click **I Agree**.
7. On the WinPcap installer **Installation options** dialog box, click **Install**.
8. On the WinPcap installer dialog, click **Finish**.
9. Repeat this procedure on the Remote Geographic Node server.

Verifying services are ready for High Availability

About this task

Verify that all CCMS and CCT services stop before you configure High Availability. This ensures that all resources are available to the Active Server when it starts.

Perform this procedure on the Active and Remote Geographic Node servers.

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**.
3. On the **CCMS** tab, check that all services are stopped.
4. If any service is running, click **Stop CCMS**.

5. On the **CCT** tab, check that all services are stopped.
6. If any service is running, click **Stop CCT**.
7. Close the System Control and Monitor Utility window.
8. Repeat this procedure on the Remote Geographic Node server.

Configuring High Availability on the Active Server

About this task

Configure High Availability resiliency on the Active Server using the High Availability Utility. The Active Server is the co-resident CCMS and CCT server that normally processes calls.

Procedure

1. Select one co-resident CCMS and CCT server to be the active server and log on.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.
4. Double-click **Server Mode**.
5. Under **Server Mode Configuration**, select **Active**.
6. Under **IP Configuration**, type the **CLAN** and **ELAN** IP addresses.
7. Under **IP Configuration**, type the **Active Server details**, **CLAN** and **ELAN** IP addresses.
8. Under **IP Configuration** type the **Standby Server details**, **CLAN** and **ELAN** IP addresses.
9. Under **IP Configuration**, type the **Managed IP** address.
10. In the **Address** box, type the IP address of the **Trusted IP** server.
11. In the **Address** box, type the IP address of the **Remote Geographic Node**.
12. Click **OK**.
    A system message box appears. You must stop the system before you save any information.
13. Click **Yes** to stop the system.

Important:

Enter the ELAN IP information only if the system has an Embedded LAN (ELAN) subnet configured. Once you enter the ELAN IP information in the High Availability Utility, you cannot switch back to a single subnet system. In order to

successfully achieve this, you must switch back to a single subnet system before High Availability is configured.

Variable definitions

Name	Description
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 Address	Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
Managed IP	The virtual Managed IP (MIP) address that is used by the Active Server for campus resiliency. The Active Server is always 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 occurred because the IP address does not change. A MIP is used only when the Active and Standby servers are in the same subnet.
Remote Geographic Node	The IP address of the Remote Geographic Node server.

Configuring E-mail notification on the Active Server

Before you begin

- If anonymous users are allowed, a user name and password may not be required. Check with the Administrator of the e-mail server for setup configuration.

About this task

If an automatic switchover occurs, the High Availability utility can send e-mail messages to configured users at a defined interval.

The default e-mail notification character set is US_ASCII. The following character sets are also supported:

- ISO-8859-1
- UTF-8
- UTF-16BE
- UTF-16LE
- UTF-16

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.
4. Double-click **Notification**.
5. Select the **Email** check box.
6. Type the **SMTP Server** name.
7. Type the **Username**.
8. Type the **Password**.
9. Type the **From Address**.
10. Type the **To Address** or **Addresses**'
11. Click **OK** to save the data.

Variable definitions

Name	Description
Email	Enables or disables e-mail notifications.
SMTP Server	The SMTP Server name, which is automatically verified when saving the data.
Username	E-mail User log on name.
Password	E-mail User log on 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.

Configuring service monitoring on the Active Server

About this task

The High Availability feature monitors a number of critical services on the Active Server. If these critical services stop or fail, they automatically restart in the correct order.

Critical services are listed, monitored, restarted, and controlled using the Contact Center Configuration tab on the Tasks tab of the High Availability utility. The Contact Center Configuration tab lists the critical CCMS services and all of the CCT services on the co-resident CCMS and CCT server.

There is no requirement to change the data in this table, the default values are suitable for most solutions.

The RestartThreshold is the time period within when the services are monitored and the counters are increased when services fail. When this threshold is met, the counters are reset to zero, monitoring restarts, and the restart threshold timer resets.

Procedure

1. Log on to the Active Server.
2. Choose **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. In the **High Availability** window, in the left pane, expand the **Tasks** folder.
4. Double-click **CC Configuration**.
5. For each service to monitor, select the **Monitor** check box.
6. For each service to restart, select the **Restart** check box.

   Important:

   By default service monitoring is selected for CCT and is not selected for CCMS.
7. In the **Start Wait Time** column, type the number of seconds to wait before restarting a service.
8. For CCT only, in the **Stop Wait Time** column, type the number of seconds to wait before stopping a service.
9. In the **Restart Limit** column, type the maximum number of attempts to restart the service before switchover occurs.This Administrator decides the maximum number.
10. In the **Restart Threshold** column, type the time in seconds to reset the restart counter (for each service that is restarted) after the threshold is passed.

Variable definitions

Name	Description
CC	The Contact Center application name, CCMS or CCT in this case, because CCMS and CCT are co-resident.
Service	The application service name, for example OAM_Service.
Monitor	Used to enable or disable the service monitoring.
Restart	Restart the service if it stops.
Start Wait Timer	The time in seconds that service monitor waits before attempting to 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. For example, if service monitor stopped this service, service monitor checks the status if the status is not SERVICE_STOPPED, it waits for Stop Wait Time before attempting to start the service.
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.

Procedure job aid

This section provides an example of the service monitor configuration in the High Availability Utility.

When the CCMS OAM service has stopped 3 times for longer than 60 seconds in a period of 12 hours, initiate an automatic switchover. This requirement is achieved by setting the OAM service configuration values to the following settings:

CC	CCMS

Service	OAM_Service
Monitor	Selected
Restart	Selected
Start Wait Timer	60 Seconds
Restart Limit	3
Restart Threshold	43200 Seconds (12 hours)

Backing up the database on the Active Server

About this task

The Active Server is configured for High Availability. Now the Remote Geographic Node server must be prepared for High Availability resiliency. Back up the Active Server to create a snapshot of the database which is then restored to the Remote Geographic Node server. On the active co-resident server all databases must be backed-up.

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
3. Click **Backup Locations**.
4. Click **Create**.
5. From the **Driver Letter** list, select the network drive on which you want to store the Contact Center Manager Server, CCT and ADMIN databases.
6. In the **UNC Path** box, type the location to store the backup, in the format \\Computer Name\Backup Location. This location must be a shared folder with correct permissions.

   Important:

   If your contact center includes Contact Center Multimedia as a standalone server, do not use the same backup folder for your co-resident and multimedia ADMIN databases, as ADMIN databases stored in the same backup location overwrite each other.
7. In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box. The user name is in the format Computer Name\Account Name.
8. In the **Password** box, type the Windows password.
9. Click **OK**.

10. In the left pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Disk**.
12. In the **Applications** section, select **CCMS**, **CCT** and **ADMIN**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **Backup**.

Restoring the database on the Remote Geographic Node server

Before you begin

- Know the location of the backup database.
- Stop all Contact Center services using the SCMU utility, if services are running.
- Ensure the patch level on the Remote Geographic Node server is the same as the Active Server.

Important:

Not all CCT data is stored in the database; therefore the following data must be configured on the Remote Geographic Node server, the CCT Communication Server 1000 service provider, CCT License, CCT Contact Management Framework, CCT SOA configuration and CCT logging location. For information about CCT commissioning, see Communication Control Toolkit commissioning for Contact Center on page 219.

Important:

You must restore all databases in a co-resident server. Restoring only CCMS and not CCT or ADMIN may leave an inconsistent server and HA cannot shadow data correctly.

Important:

Restoring the Admin database can change configuration of Backup locations on the Remote Geographic Node server if the Active Server and Remote Geographic Node server backup locations are different. Therefore, after you restore the ADMIN database, close and reopen the Database and Maintenance utility.

Important:

The Server Configuration utility must be run after a database restore has been performed and the administrator must check the data to ensure that it is correct.

About this task

Restore the database from the Active Server to the Remote Geographic Node server to ensure the databases are consistent. The Database Maintenance utility can restore only one application database at a time. Restore the data for the CCMS, CCT, and ADMIN databases

You must restore the CCMS, CCT, and ADMIN database onto the Remote Geographic Node server. You must restore the ADMIN database last.

Procedure

1. Log on to the Remote Geographic Node server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
3. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
4. In the right pane, under **Media Type**, select the media type on which the backup is restored.
5. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
6. Under **Application**, select the database to restore, either **CCMS**, **CCT** or **ADMIN**.
7. Under **Restore contents**, select **Data**.
8. Click **Restore**.
9. Use the **Progress information** field to monitor the progress of the restoration.
10. Repeat steps 6 to 8 to restore all databases.
11. Click **Exit** to close the Database Maintenance utility.

Variable definitions

Name	Description
Application	The database and applications of Contact Center that you can back up.
Backup Location	The destination of the network disk. The values are configured in the Backup Locations.
Restore contents	The type of content that is stored in the database. Data is in the database. Schema is the data for the database structure, tables and procedures.

Name	Description
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.

Configuring server details on the Remote Geographic Node server

Before you begin

- The Active Server databases are restored on to the Remote Geographic Node server.

About this task

After you restore the Active Server database on to the Remote Geographic Node server, the Remote Geographic Node server database contains the same agent and statistical data as the Active Server. However the Remote Geographic Node server details are now also configured exactly the same as the Active Server, and you must therefore reconfigure the Remote Geographic Node server with its own server details.

Important:

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

Procedure

1. Log on to the Remote Geographic Node server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
3. In the **Server Configuration** dialog box, click the **Local Settings** tab.
4. Update the Remote Geographic Node server local settings.
5. Click **Apply All**.
6. In the **Server Configuration** dialog box, click the **Licensing** tab.
7. Update the Remote Geographic Node server licensing details.
8. Click **Apply All**.
9. Click **OK**.

10. If your contact center is AML-based, in the **Server Configuration** dialog box, click the **Switch CS 1000** tab.
11. Update the Avaya Communication Server 1000 PABX Data details.
12. Click **Apply All**.
13. Click **OK**.
14. If your contact center is SIP-enabled, in the **Server Configuration** dialog box, under **SIP**, click the **Network Settings** tab.
15. Update the Remote Geographic Node server **SIP Network Settings** details.
16. Click **Apply All**.
17. Click **OK**.
18. If your contact center is SIP-enabled, in the **Server Configuration** dialog box, under **SIP**, click the **Local Subscriber** tab.
19. Update the Remote Geographic Node server **SIP Local Subscriber** details.
20. Click **Apply All**.
21. Click **OK**.
22. Click **Exit**.

Variable definitions

Name	Description
Avaya Server Subnet IP Address	The IP address of the subnet that connects the Contact Center servers (Contact Center Manager Server, Network Control Center, Contact Center Manager Administration, and Contact Center Multimedia).
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.

Name	Description
CallPilot Alternative Port	The port number of the alternate Avaya CallPilot® voice connection type to the Contact Center Manager Server when working with an Avaya Communication Server 1000 PABX. The default port number is 5060.
CallPilot IP Address	The IP address of the primary Avaya CallPilot® voice connection type to the Contact Center Manager Server when working with an Avaya Communication Server 1000 PABX.
CallPilot Port	The port number of the primary Avaya CallPilot® voice connection type to the Contact Center Manager Server when working with an Avaya Communication Server 1000 PABX. The default port is 5060.
PABX Customer Number	The customer number for the PABX.
PABX IP Address	The IP address of the PABX.
PABX Name	The name of the Avaya Communication Server 1000 PABX. Valid characters for PABX names are A-Z, a-z, 0-9, underscore (_), and period (.). PABX names must begin with an alphabetical character and cannot contain spaces. The last character must not be an underscore or period. PABX names must not exceed 80 characters in length.
Voice Proxy Server • IP or FQDN • Port • Network Transport	Information about the server that provides support for inbound and outbound calls, such as routing a call to an agent telephone. If the contact center uses an Avaya Communication Server 1000 Network Routing Service (NRS), enter the IP address or Fully Qualified Domain Name (FQDN) for it here. If the contact center uses an Avaya Aura® Session Manager, enter the IP address or Fully Qualified Domain Name (FQDN) for the primary Session Manager here. If the contact center uses an Avaya Aura® SIP Enablement Services (SES) server, enter the IP address or Fully Qualified Domain Name (FQDN) for it here.

Name	Description
	The server listening port. The default port is 5060. The SIP Network Transport communication protocol. Avaya recommends that you use TCP for Avaya Communication Server 1000.
CTI Proxy Server • IP or FQDN • Port • Network Transport	Information about the server that provides support for SIP Computer Telephony Integration (CTI) so that Agent Desktop can acquire and control agent telephones for TR87. If the contact center uses an Avaya Communication Server 1000 Signaling Server, enter the IP address or Fully Qualified Domain Name (FQDN) for it here. If the contact center uses an Avaya Aura® Application Enablement Services server, enter the IP address or Fully Qualified Domain Name (FQDN) for it here. For an Avaya Communication Server 1000 the default SIP CTI Proxy Server port is 5060. For an Application Enablement Services server the default SIP CTI Proxy Server port is 4723. The SIP Network Transport communication protocol. For an Avaya Communication Server 1000, the default Network Transport communication protocol is TCP. For an Application Enablement Services server, the default Network Transport communication protocol is TLS.
Backup Voice Proxy Server • IP or FQDN • Port • Network Transport	Information about the server that provides backup support for inbound and outbound calls, such as routing a call to an agent telephone. Avaya Aura® Contact Center must have a Standby Server license to support a Backup Voice Proxy Server. The only type of Backup Voice Proxy Server supported by Avaya Aura® Contact Center is an Avaya Aura® Session Manager when it used with an Avaya Aura® Communication Manager. If the contact center uses an Avaya Aura® Communication Manager and a backup Session Manager, enter the IP address or

Name	Description
	Fully Qualified Domain Name (FQDN) for the backup Session Manager here. The server listening port. The default port is 5060. The Backup Voice Proxy Server transport protocol.
IM Proxy Server • IP or FQDN • Port • Network Transport	Information about the server that supports the deployment of Instant Message over SIP. From the IM Provider list, select the name of the instant messaging provider. Select either Aura Presence Services or Microsoft OCS. The IP address or Fully Qualified Domain Name (FQDN) of the SIP IM Proxy Server. The default SIP IM Proxy Server port is 5222. The IM SIP Proxy Server transport protocol.
IM Provider	Select your IM Provider, Microsoft OCS or Aura Presence Services.
XMPP Domain	If using an Avaya Aura® Presence Services server, enter the domain name of the Extensible Messaging and Presence Protocol (XMPP) server.
Local SIP Subscriber • Contact Center Name • Domain Name • Password	Information about the environment of the SIP-enabled contact center and how to identify the server within the network. The registration user name on the registration proxy. Use a suitable user name following the standards in your system. Associated domain name for the SIP-enabled contact center. Password for the registration user name.
Web Service Ports	The Web Service Ports group box appears only if you select Avaya Aura® Presence Services as the IM Provider. Server Port default is 9100 Client Port default is 9120
SIP Server Type	Type of SIP proxy for the contact center integration. Depending on the switch type you select in the Application Selection window, the system

Name	Description
	automatically sets the specific SIP Server Type as the default. • For SIP Avaya Aura® 6.1 switch type, the default SIP Server Type is Avaya Aura® 6.1. • For SIP Avaya Communication Server 1000 switch type, the default SIP Server Type is CS1000.
MS Locale	Locale (including language and dialects) of the system environment.
Local Listening Ports	The SIP Communication protocol accepted by the system for incoming calls. TCP/UDP Port default is 5060 TLS Port default is 5061

Configuring High Availability on the Remote Geographic Node server

Before you begin

- The Active Server databases are restored on to the Remote Geographic Node server.

About this task

Configure High Availability resiliency on the Remote Geographic Node server using the High Availability utility. The co-resident CCMS and CCT Standby Server shadows the Active Server and takes over processing if the Active Server fails.

Procedure

1. Log on to the Remote Geographic Node server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. In the left pane of the **High Availability** dialog box, click **Server Mode**.
4. In the **Server Mode Configuration** section, select **Standby**.
5. Under **IP Configuration**, type the **CLAN** and **ELAN** IP addresses.
6. Under **IP Configuration**, type the **Active Server details**, **CLAN** and **ELAN** IP addresses.
7. Click **OK**.

A system message box appears. You must stop the system before you save any information.

8. Click **OK**.

Variable definitions

Name	Description
Active Server details	The Managed IP address for the server initially configured in Active mode. Enter the Managed IP address of the Active server in the campus site. Enter the Managed IP address of the campus co-resident server here. If the Active server fails the Remote Geographic Node uses the Managed IP address to continue shadowing the Standby server in the campus site.
Trusted IP Address	Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.

Starting the Active Server

About this task

Start the Active Server using the High Availability utility. Starting the Active Server starts CCMS, CCT, and system processes.

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Tasks**.
4. Double-click **CC Applications**.
5. In the first box under **CC Applications**, select the system.
6. Click **Start**.

A delay occurs before all Contact Center services start.

7. Click **OK**.
8. To verify that the Contact Center services are running using the SCMU, select **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**. Check the CCMS and CCT services are running.

Starting shadowing on the Remote Geographic Node server

Before you begin

Important:

It is advisable on the Remote Geographic Node server not to stop and start shadowing but to use the pause and resume functionality.

About this task

Start shadowing on the Remote Geographic Node server using the High Availability utility. While the Remote Geographic Node server is shadowing the Active server, it maintains a near real-time local copy of the CCMS, CCT, and Administration databases.

Important:

You must backup the Active server database, restore it onto the Standby server, and enable shadowing within 24 hours. If the difference in time between the Active and Standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the Active server database and restore it onto the Standby server before re-enabling shadowing. Ensure that the system clock time on the Active and Standby servers are synchronized.

Procedure

1. Log on to the Remote Geographic Node server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Tasks**.
4. Double-click **System Control**.
5. In the **Control** box, select **Shadowing**.
6. Click **Start**.
7. Click **OK**.

8. To verify that the CCMS services are stopped using the SCMU, select **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**. Check the CCMS services are stopped.
9. To verify that the CCT services are running using the SCMU, select **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**. Check the CCT services are running.

Verifying shadowing is running on the Active Server

About this task

Verify that the Remote Geographic Node co-resident CCMS and CCT server is shadowing the Active server using the High Availability Utility. The System dialog box of the High Availability utility displays system information about the Active and the Remote Geographic Node servers.

The dialog box displays the followings information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information
- License information
- Databases shadowed
- Time of last record shadowed
- Database namespaces
- Local and remote information on system status, switchover, shadowing and network.
- CC Application install information
- Database space and journaling information
- Database processes information

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. In the left pane, expand **Configuration**.

4. Select **System**.
5. Select **Get System Configuration**.
   The most recent system information appears.

Chapter 26: High Availability campus CCMM commissioning

This section describes how to configure High Availability (HA) resiliency on a pair of standalone Contact Center Multimedia (CCMM) servers in a campus contact center solution.

High Availability CCMM commissioning overview:

In a High Availability Campus server configuration, one CCMM server is the active server and one is the standby server. The active CCMM server actively processes contacts. The standby server shadows the active server. The standby server copies all configuration changes made on the active server and monitors the active server status. If the active CCMM server fails, the standby CCMM server, running in standby mode, recognizes the failure and starts processing contacts. The active and standby CCMM servers are part of the same contact center and they must be in the same subnet IP address range for campus High Availability resiliency to work.

You must configure the standby CCMM server the same as the active server. The standby and active servers must have the same patch level and the same hard disk drive partitions. Configuration changes made to the active CCMM server during normal operation are automatically copied to the standby server so that the standby server can take over processing from the active server when necessary.

In a campus solution, a CCMM hardware, network, or database failure can initiate a switchover but only if:

- The switchover check box on both CCMM servers is selected
- The standby CCMM server is shadowing the active server
- A valid license file containing standby server license information for CCMM exists to allow switchover

Managed IP Address:

A Managed IP (MIP) address is a virtual IP address that is attached to a network adapter on the active server. Each Avaya Aura® Contact Center application server is assigned a static IP address. After the active server in each replication pair is determined, the active server attaches a Managed IP address to its network interface. The managed IP address is assigned only to the active server and it is used by all other Contact Center applications and clients to connect to that application. The standby server assumes this same managed IP address only 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.

High Availability Utility:

High Availability resiliency for Contact Center Multimedia is configured using the High Availability Utility in the Database Utilities. Use the High Availability Utility to configure which server is the active and which is the standby server. The HA utility also configures the Managed IP of the active server.

The High Availability Utility on an Active Server has the following information configured on the Configuration tab:

- Server Mode
  - Configure the IP address for the Active and Standby servers
  - Configure the IP address for Trusted servers
  - Configure the IP address for the Remote Geographic node
  - Identify the Active or Standby server
  - Enable Automatic Switchover
  - Configure the switchover time-out: the wait time if a network outage occurs before an automatic switchover occurs
- Notifications
  - Configure an e-mail server to allow for e-mail notifications
  - Configure where and how often to send e-mail notifications
  - Configure the e-mail character set
- System
  - Display information on the system status
  - Verify that shadowing is running

The High Availability utility on an Active Server has the following dialogs under the Tasks tab:

- CC Applications
  - Start or stop the system
  - Enable or disable CC applications
  - Display system information
- CC Configuration
  - Monitor application service status
- System Control
  - Initiate a manual switchover for the Active Server
  - Initiate Standby Server shadowing

Prerequisites

- Ensure unused Network Interface Cards (NICs) are disabled.
- Install CCMM software on the active server. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- Commission Contact Center Multimedia. See Contact Center Multimedia server commissioning on page 237.
- Know how to back up the Contact Center Multimedia database. See *Avaya Aura® Contact Center Server Administration* (NN44400-610).
- Know how to restore the Contact Center Multimedia database. See *Avaya Aura® Contact Center Server Administration* (NN44400-610).
- Know how to configure the High Availability settings.
- Install Contact Center Multimedia software on the standby server. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCMM stores license information in the registry. Configure CCMM licensing on the standby CCMM server, after restoring the database from the active server. See Contact Center Multimedia server commissioning on page 237.

High Availability CCMM commissioning procedures

About this task

This task flow shows the sequence of procedures performed to commission High Availability for CCMM.

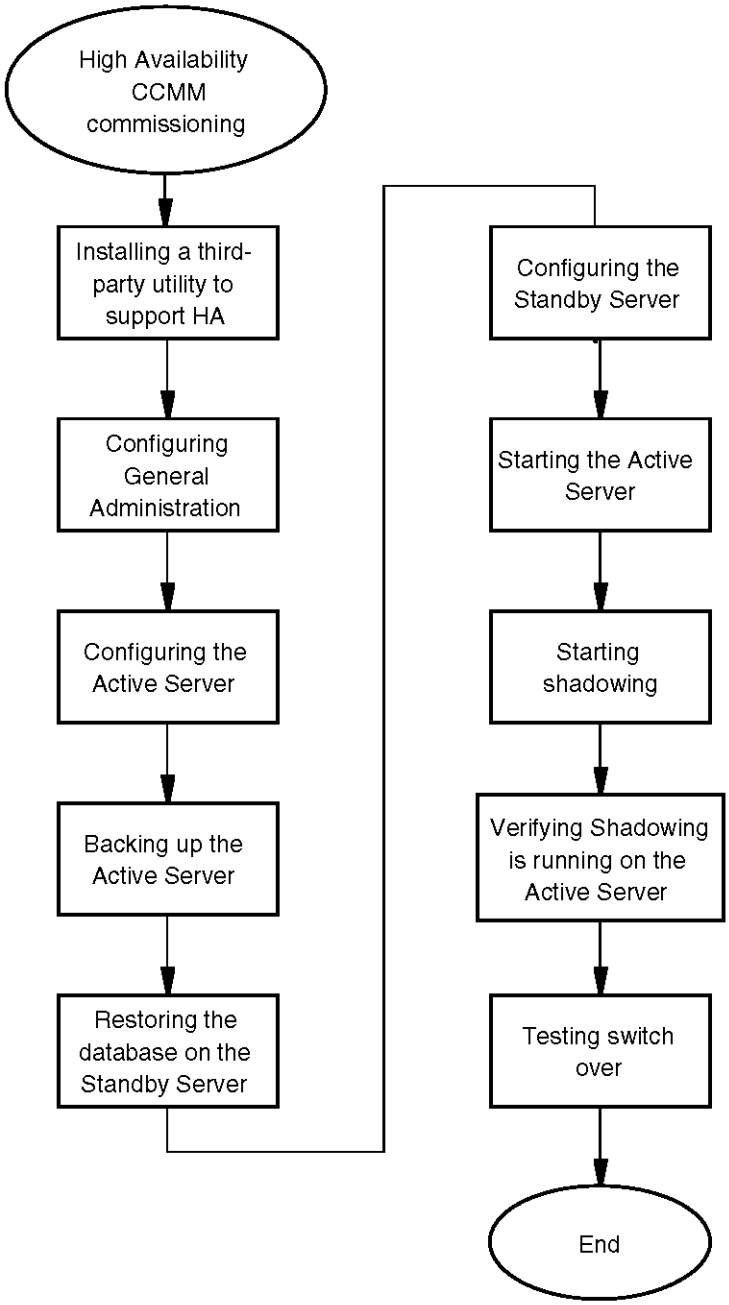


Figure 55: High Availability CCMM commissioning procedures

Installing a third-party utility to support High Availability

About this task

Install a third-party utility required by the Avaya Aura® Contact Center High Availability feature.

Perform this procedure on the Active and Standby servers.

Procedure

1. Log on to the Active Server.
2. Retrieve the WinPcap installer from a CCMS server.

   The WinPcap installer is located at: <*installation drive*>:\Avaya \Contact Center\Manager Server\CCSMMC\thirdparty\winpcap.
3. Save it on the CCMM server you are commissioning.
4. On the CCMM server, using Windows Explorer, navigate to the location you had saved the WinPcap_4_1_2.exe file in step 3.
5. Double-click **WinPcap_4_1_2.exe**.
6. On the WinPcap installer dialog, click **Next**.
7. On the WinPcap installer Setup Wizard dialog, click **Next**.
8. On the WinPcap installer License Agreement dialog, click **I Agree**.
9. On the WinPcap installer Installation options dialog, click **Install**.
10. On the WinPcap installer dialog, click **Finish**.
11. Repeat this procedure on the Standby Server.

Configuring CCMM General Administration

Before you begin

- Log on to the Contact Center Manager Administration application.

About this task

In a multimedia-enabled solution Avaya Aura® Agent Desktop client software is typically downloaded from a Contact Center Multimedia (CCMM) server. Avaya Aura® Agent Desktop then communicates with that Contact Center Multimedia server to handle e-mail based

contacts. Avaya Aura® Agent Desktop communicates with a Communication Control Toolkit (CCT) server to handle voice contacts.

In a multimedia-enabled High Availability solution, use the CCMM Administration tool to configure standby CCMM and CCT server details. Avaya Aura® Agent Desktop client software downloads these standby server details and communicates with these standby servers, if it cannot communicate with the active CCMM or CCT servers.

Important:

Changes to the CCMM Server Settings may require a CCMM server restart before they take effect.

Procedure

1. Click **Multimedia**.
2. In the left column, select **General Administration**.
3. Click **Server Settings**.
4. Ensure that **Contact Center Manager Server** is configured with the managed IP address or managed name of the CCMS High Availability pair.
5. Ensure that **Contact Center License Server** is configured with the managed IP address or managed name of the CCMS High Availability pair, assuming that the License Managers are installed co-resident with the CCMS servers.
6. Ensure that **Contact Center Manager Administration** is configured with the managed name of the CCMA High Availability pair.
7. Ensure that **Contact Center Multimedia Server** is configured with the Managed IP address or managed name of the CCMM High Availability pair.
8. If your solution has a Remote Geographic Node CCMM server, enter its name or IP address in the **Contact Center Multimedia Standby Server** box. If your solution does not have a Remote Geographic Node CCMM server, then leave the Contact Center Multimedia Standby Server not configured.

   Note:

   The Contact Center Multimedia Standby server is configured only when the solution has a Remote Geographic Node CCMM server.
9. Configure the **Communication Control Toolkit Server**.
10. Configure the **Standby CCT Server**.
11. If you are using a Remote Geographic Node server, configure the **Geographic Alternate CCT Server**. If the Geographic Alternate CCT Server does not exist, click **New** to create one.
12. Configure **CC Web Stats**. If the Contact Center Web Statistics Server details do not exist and if you have Web Statistics, click **New** to create one.
13. In the left column select **Email**.

14. Click **General Settings**.
15. Ensure that the Inbound URL is of the form `http://<ManagedIPAddress>/inboundattachment`.
16. Ensure that the Outbound URL is of the form `http://<ManagedIPAddress>/outboundattachment`.

Variable definitions

Name	Description
Contact Center Manager Server	Enter the Managed IP address or managed name of the CCMS High Availability server pair.
Contact Center Multimedia Server	Enter the Managed IP address or managed name of the CCMM High Availability server pair.
Contact Center Multimedia Standby Server	Enter the IP address or name of the Remote Geographic Node CCMM server, if your solution has one.
Communication Control Toolkit Server	If you are using an Avaya Aura® Communication Manager Release 6.0.1 or later and an Avaya Aura® Session Manager, in the Communication Control Toolkit Server box, enter the name or IP address of your primary CCT server. OR If you are using one of the following: • Avaya Communication Server 1000 • Avaya Aura® SIP Enablement Services server • Avaya Aura® Midsize Business Template in the Communication Control Toolkit Server box, enter the Managed IP address of the CCT High Availability pair.
Standby CCT Server	If you are using an Avaya Aura® Communication Manager Release 6.0.1 or later and an Avaya Aura® Session Manager, enter the name or IP address of your standby CCT server. OR If you are using one of the following: • Avaya Communication Server 1000 • Avaya Aura® SIP Enablement Services server • Avaya Aura® Midsize Business Template leave the Standby CCT Server input blank.
Geographic Alternate CCT Server	Enter the name or IP address of the Remote Geographic Node CCT server.

Name	Description
CC Web Stats	The Managed IP address or managed name of the optional Web Statistic server that agents and supervisors use to view real-time statistics for call handling, skillset data, and the state information on the Agent Desktop. This is typically the Managed IP address or managed name of the CCMS server.

Configuring the Active Server

About this task

The Active Server is configured using the High Availability utility. This utility saves IP information for the Active Server to the database.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
2. Expand **Configuration**.
3. Double-click **Server Mode**.
4. Under **Server Mode**, select **Active**.
5. Under **Server Mode Configuration**, in the text box, type the maximum length of time the network connectivity tests can continue to fail consecutively before corrective action is considered.
6. Under **Server Mode Configuration**, from the drop down list, select the unit of time for the network connectivity tests.
7. Under **IP Configuration**, type the **Managed IP**, **CLAN** IP address.
8. Under **IP Configuration**, type the **Active Server details**, **CLAN** IP address.
9. Under **IP Configuration**, type the **Standby Server details**, **CLAN** IP address.
10. In the **Trusted IP** box, type the IP **Address** of the trusted server.
11. In the **Address** box, type the IP address of the optional **Remote Geographic Node**.
12. Click **OK**.
    A system message box appears. You must stop the system before you save any information.
13. Click **Yes** to stop the system.
14. Click **OK** to save the data.

Variable definitions

Name	Description
Server Mode Configuration - Network Timeout	The High Availability—Network Timeout value sets the maximum length of time the network connectivity test can continue to fail consecutively, before corrective action is considered. The minimum Network Timeout value is 200 milliseconds (200ms) and the maximum Network Timeout value is 5 seconds. Avaya recommends that you set Network Timeout high enough to be tolerant of normal network latency, but low enough to be responsive if a failure occurs.
Managed IP	The Managed IP (MIP) address that is used for both the Active and Standby servers for campus resiliency. The Active Server is always 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 occurred because the IP address does not change. A MIP is used only 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 Address	The Active and Standby servers use the Trusted IP address to verify network connectivity. If the Active server cannot communicate with the Standby server it attempts to communicate with the Trusted IP address. If the Active Server cannot connect to the Trusted IP address on startup then no Contact Center services start on that server. If the Active server cannot communicate with the Trusted IP address, and if shadowing and switchover are enabled, then the Active server stops processing contacts and shuts down. The Standby server starts processing contacts if it cannot communicate with the

Name	Description
	Active server but can communicate with the Trusted IP address. Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
Remote Geographic Node	The IP address of the optional Remote Geographic Node.

Backing-up the CCMM Active Server database

About this task

Use the Database Maintenance utility to back up the Active Server database. The backup of the database is restored to the Standby Server.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
2. Click **Backup Locations**.
3. Click **Create**.
4. From the **Drive Letter** list, select the network drive on which you want to store the CCMM database.
5. In the **UNC Path** box, type the location to store the backup, in the format `\\Computer Name\Backup Location`.

   Important:

   When Contact Center Multimedia is installed as a standalone server, do not use the same backup folder for your co-resident and multimedia ADMIN databases, as ADMIN databases stored in the same backup location overwrite each other.

   This location must be a shared folder with correct permissions.
6. In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box.

   The user name is in the format `Computer Name\Account Name`.
7. In the **Password** box, type the domain password.
8. Click **OK**.

Comments? infodev@avaya.com

9. In the left pane, click **Immediate Backup**.
10. In the **Media Type** section, select **Network Disk**.
11. In the **Applications** section, select **CCMM** and **ADMIN**.
12. From the **Backup Location** list, select the network drive on which to store the backup.
13. Click **OK**.

Restoring the database on the Standby Server

Before you begin

- When CCMM is installed, the license type is NODAL. If you have a Corporate (CORP) license this must be set on the standby server, before the active server backup is restored on to the standby machine.

Important:

Restore the CCMM database first and then the ADMIN database.

Important:

Restoring the ADMIN database can change configuration of Backup locations on the Standby Server, if the Active Server and Standby Server backup locations are different. After you restore the ADMIN database, close and reopen the Database and Maintenance utility.

About this task

Restore the database from the Active Server to the Standby Server to ensure the databases are consistent. The Database Maintenance utility can restore only one application's data at a time. Therefore restore the data for the CCMM and ADMIN databases.

You must restore the CCMM and ADMIN databases to the Standby Server. Restore the ADMIN database last.

Procedure

1. Log on to the Standby Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
3. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
4. In the right pane, under **Media Type**, select the media type on which the backup is restored.

5. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
6. Under **Application**, select the database to restore.
7. Under **Restore contents**, select **Data**.
8. Click **OK**.
9. Use the **Progress information** field to monitor the progress of the restoration.
10. Click **Exit** to close the Database Maintenance utility.

Configuring the Standby Server

Before you begin

- The database from the Active server has been restored to the Standby Server.

About this task

Configure the Standby Contact Center Multimedia (CCMM) server. The Standby CCMM server must be shadowing the Active CCMM server for switchover to occur, if the Active server fails. While the Standby server is shadowing the Active server, it maintains a near real-time local copy of the CCMM and Administration databases. Therefore, the Standby Server is configured with the most recent data and it can take over from the Active Server if necessary.

Procedure

1. Log on to the Standby Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. In the left pane, click **Server Mode**.
4. In the **Server Mode Configuration** section, select **Standby**.
5. Under **IP Configuration**, type the **Active Server details**, **CLAN** IP address.
6. Under **IP Configuration**, type the **Standby Server details**, **CLAN** IP address.
7. Under **IP Configuration**, under **Trusted IP**, type the Trusted IP address.
8. Under **IP Configuration**, under **Remote Geographic Node**, type the optional Remote Geographic Node IP address.
9. Click **OK**.
   A system message box appears. You must stop the system before you save any information.

10. Click **OK**.

Starting the Active Server

About this task

Start the Active Server using the CC Applications tab in the High Availability utility. Starting the Active Server starts the system processes.

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.
4. Under **Server Mode Configuration**, select **Switchover**.
5. Expand **Tasks**.
6. Double-click **CC Applications**.
7. In the first box under **CC Applications**, select the system.
8. Click **Start**.
9. Click **OK**.

Starting shadowing on the Standby Server

About this task

Use the High Availability utility to start shadowing on the Standby Server.

Important:

You must backup the Active server database, restore it onto the Standby server, and enable shadowing within 24 hours. If the difference in time between the Active and Standby server database content is greater than 24 hours then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the Active server database and restore it onto the Standby server before re-enabling shadowing. Ensure that the system clock time on the Active and Standby servers are synchronized.

Procedure

1. Log on to the Contact Center Multimedia standby server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.
4. In **Server Mode Configuration**, select **Switchover**.
5. Under **Tasks**, click **System Control**.
6. Beside **Control**, select **Shadowing**.
7. Click **Start**.

Verifying shadowing is running on the Active Server

About this task

The system information tab of the High Availability utility displays system information regarding the Active and the Standby servers. The dialog box displays the following information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status
- Remote server port information
- Licencse information
- Databases shadowed
- Time of last record shadowed
- Database namespaces
- Local and remote information on system status, switchover, shadowing, and network.
- CC Application install information
- Database space and journaling information
- Database processes information

Use this procedure to verify the settings.

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.
4. Select **System**.
5. Select **Get System Configuration**.
   The most recent system information appears.
6. Under the **Shadowing** section, view the time of the most recent shadowed record.

   Ensure it has an up-to-date time, which corresponds with when shadowing was started.

Testing a switchover on the CCMM solution

About this task

When the CCMM server commissioning is complete, you can test the CCMM switchover to ensure that it works.

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. On the Active Server, select **System Control**.
4. Under **Control**, select **Switchover** to initiate a manual switchover.
5. Send a test e-mail to one of the CCMM configured mailboxes.
   After the e-mail is received on the new Active Server, the test is successfully completed.

Chapter 27: Geographic High Availability CCMM commissioning

This section describes how to configure geographic High Availability for pair of standalone Contact Center Multimedia (CCMM) servers in a geographic Wide Area Network solution.

In geographic Wide Area Network solutions the standby server on the remote geographic site is called a Remote Geographic Node server. The Active CCMM server and the Remote Geographic Node CCMM server are part of the same Avaya Aura® Contact Center solution but they are typically in different geographic locations and subnets.

The Active CCMM server may also have a local standby CCMM server in the same campus location. The standby CCMM server shadows the Active CCMM server. If the Active CCMM server fails the local standby CCMM server takes over call processing on the local site.

The Remote Geographic Node CCMM server on the remote site shadows the Active server on the campus site. If the Active server fails, the local standby server assumes the shared Managed IP address and starts processing calls. The Remote Geographic Node server monitors the campus Managed IP address so it continues shadowing.

Geographic High Availability CCMM commissioning overview:

In a geographic High Availability server configuration, one CCMM server is the active server and one server is the Remote Geographic Node. The active CCMM server actively processes contacts. The Remote Geographic Node server shadows the active server. The Remote Geographic Node server copies all configuration changes made on the active server and monitors the active server status. If the active CCMM server fails, the Remote Geographic Node CCMM server does not start processing contacts. You must start the Remote Geographic Node server manually.

You must configure the Remote Geographic Node CCMM server the same as the active server. The Remote Geographic Node and active servers must have the same patch level and the same hard disk drive partitions.

Prerequisites

- Ensure unused Network Interface Cards (NICs) are disabled.
- Install CCMM software on the active server. See *Avaya Aura® Contact Center Installation* (NN44400-311).

- Commission Contact Center Multimedia. See Contact Center Multimedia server commissioning on page 237.
- Know how to back up the Contact Center Multimedia database. See *Avaya Aura® Contact Center Server Administration* (NN44400-610).
- Know how to restore the Contact Center Multimedia database. See *Avaya Aura® Contact Center Server Administration* (NN44400-610).
- Know how to configure the High Availability settings.
- Install Contact Center Multimedia software on the Remote Geographic Node server. See *Avaya Aura® Contact Center Installation* (NN44400-311).
- CCMM stores license information in the registry. Configure CCMM licensing on the Remote Geographic Node CCMM server, after restoring the database from the active server. See Contact Center Multimedia server commissioning on page 237.

Geographic High Availability CCMM commissioning procedures

About this task

This task flow shows the sequence of procedures performed to commission Geographic High Availability for CCMM.

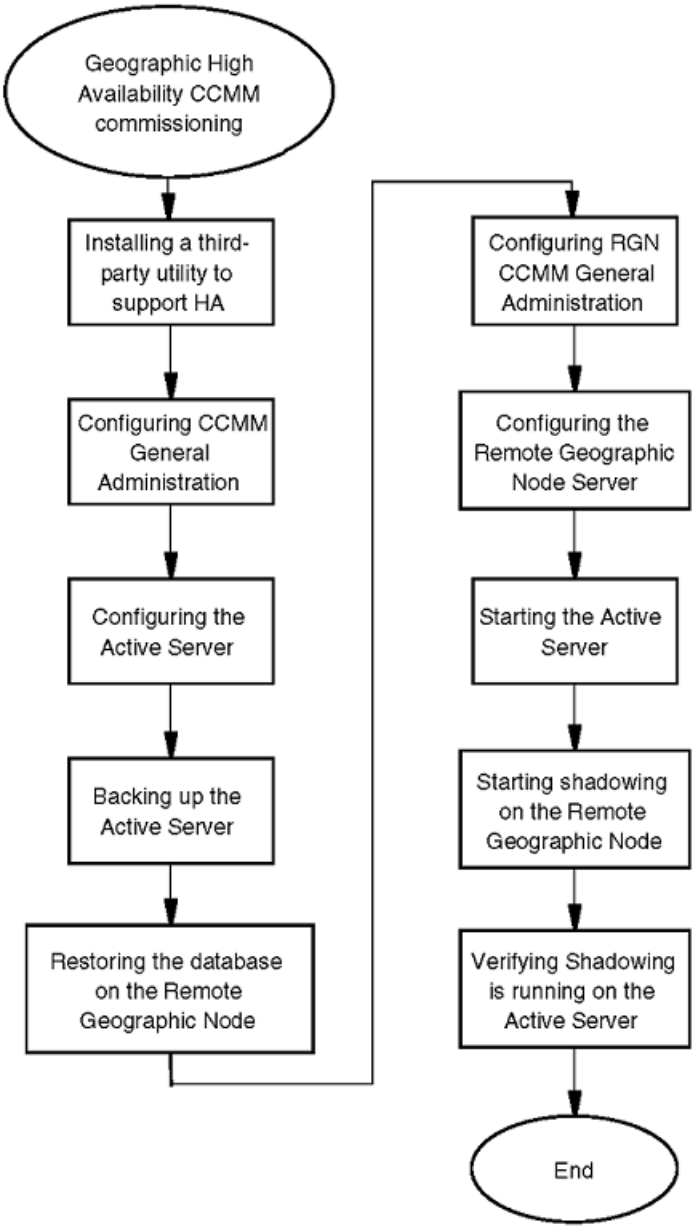


Figure 56: Geographic High Availability CCMM commissioning procedures

Installing a third-party utility to support High Availability

About this task

Install a third-party utility required by the Avaya Aura® Contact Center High Availability feature.

Perform this procedure on the Active and Remote Geographic Node servers.

Procedure

1. Log on to the Active Server.
2. Retrieve the WinPcap installer from a CCMS server.

   The WinPcap installer is located at: <*installation drive*>:\Avaya \Contact Center\Manager Server\CCSMMC\thirdparty\winpcap.
3. Save it on the CCMM server you are commissioning.
4. On the CCMM server, using Windows Explorer, navigate to the location you had saved the WinPcap_4_1_2.exe file in step 3.
5. Double-click **WinPcap_4_1_2.exe**.
6. On the WinPcap installer dialog, click **Next**.
7. On the WinPcap installer Setup Wizard dialog, click **Next**.
8. On the WinPcap installer License Agreement dialog, click **I Agree**.
9. On the WinPcap installer Installation options dialog, click **Install**.
10. On the WinPcap installer dialog, click **Finish**.
11. Repeat this procedure on the Remote Geographic Node Server.

Configuring CCMM General Administration

Before you begin

- Log on to the Active CCMM server.
- Log on to the Contact Center Manager Administration application of the Active server.

About this task

In a multimedia-enabled solution Avaya Aura® Agent Desktop client software is typically downloaded from a Contact Center Multimedia (CCMM) server. Avaya Aura® Agent Desktop then communicates with that Contact Center Multimedia server to handle e-mail based

contacts. Avaya Aura® Agent Desktop communicates with a Communication Control Toolkit (CCT) server to handle voice contacts.

In a multimedia-enabled High Availability solution use the CCMM Administration tool to configure standby CCMM and CCT server details. Avaya Aura® Agent Desktop client software downloads these standby server details and communicates with these standby servers, if it cannot communicate with the active CCMM or CCT servers.

Important:

Changes to the CCMM Server Settings may require a CCMM server restart before they take effect.

Procedure

1. Click **Multimedia**.
2. In the left column, select **General Administration**.
3. Click **Server Settings**.
4. Ensure that **Contact Center Manager Server** is configured with the managed IP address or managed name of the CCMS High Availability pair.
5. Ensure that **Contact Center License Server** is configured with the managed IP address or managed name of the CCMS High Availability pair, assuming that the License Managers are installed co-resident with the CCMS servers.
6. Ensure that **Contact Center Manager Administration** is configured with the managed name of the CCMA High Availability pair.
7. Ensure that **Contact Center Multimedia Server** is configured with the managed IP address or managed name of the CCMM High Availability pair.
8. Ensure that **Contact Center Multimedia Standby Server** is configured with the name or IP address of the Remote Geographic Node CCMM server.
9. Configure the **Communication Control Toolkit Server**.
10. Configure the **Standby CCT Server**.
11. If you are using a CCT Remote Geographic Node server, configure the **Geographic Alternate CCT Server**. If the Geographic Alternate CCT Server does not exist, click **New** to create one.
12. Configure **CC Web Stats**. If the Contact Center Web Statistics Server does not exist, click **New** to create one.

Variable definitions

Name	Description
Contact Center Manager Server	Enter the Managed IP address or managed name of the CCMS High Availability server pair.
Contact Center Multimedia Server	Enter the Managed IP address or managed name of the CCMM High Availability server pair.
Contact Center Multimedia Standby Server	Enter the IP address or name of the Remote Geographic Node CCMM server, if your solution has one.
Communication Control Toolkit Server	If you are using an Avaya Aura® Communication Manager Release 6.0.1 or later and an Avaya Aura® Session Manager, in the Communication Control Toolkit Server box, enter the name or IP address of your primary CCT server. OR If you are using one of the following: • Avaya Communication Server 1000 • Avaya Aura® SIP Enablement Services server • Avaya Aura® Midsize Business Template in the Communication Control Toolkit Server box, enter the Managed IP address of the CCT High Availability pair.
Standby CCT Server	If you are using an Avaya Aura® Communication Manager Release 6.0.1 or later and an Avaya Aura® Session Manager, enter the name or IP address of your standby CCT server. OR If you are using one of the following: • Avaya Communication Server 1000 • Avaya Aura® SIP Enablement Services server • Avaya Aura® Midsize Business Template leave the Standby CCT Server input blank.
Geographic Alternate CCT Server	Enter the name or IP address of the Remote Geographic Node CCT server.
CC Web Stats	The Managed IP address or managed name of the optional Web Statistic server that agents and supervisors use to view real-time statistics for call handling, skillset data, and the state information on the Agent Desktop. This is typically the Managed IP address or managed name of the CCMS server.

Configuring the Active Server

About this task

The Active Server is configured using the High Availability utility. This utility saves IP information for the Active Server to the database.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
2. Expand **Configuration**.
3. Double-click **Server Mode**.
4. Under **Server Mode**, select **Active**.
5. Under **Server Mode Configuration**, in the text box, type the maximum length of time the network connectivity tests can continue to fail consecutively before corrective action is considered.
6. Under **Server Mode Configuration**, from the drop down list, select the unit of time for the network connectivity tests.
7. Under **IP Configuration**, type the **Managed IP**, **CLAN** address.
8. Under **IP Configuration**, type the **Active Server details**, **CLAN** IP address.
9. Under **IP Configuration**, type the **Standby Server details**, **CLAN** IP address.
10. In the **Trusted IP** box, type the IP **Address** of the trusted server.
11. In the **Address** box, type the IP address of the optional **Remote Geographic Node**.
12. Click **OK**.
    A system message box appears. You must stop the system before you save any information.
13. Click **Yes** to stop the system.
14. Click **OK** to save the data.

Variable definitions

Name	Description
Server Mode Configuration - Network Timeout	The High Availability—Network Timeout value sets the maximum length of time the network connectivity test can continue to fail consecutively, before corrective action is considered. The minimum Network Timeout value is 200 milliseconds (200ms) and the maximum Network Timeout value is 5 seconds. Avaya recommends that you set Network Timeout high enough to be tolerant of normal network latency, but low enough to be responsive if a failure occurs.
Managed IP	The Managed IP (MIP) address that is used for both the Active and Standby servers for campus resiliency. The Active Server is always 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 occurred because the IP address does not change. A MIP is used only 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	Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.
Remote Geographic Node	The IP address of the optional Remote Geographic Node.

Backing-up the CCMM Active Server database

About this task

Use the Database Maintenance utility to back up the Active server database. The backup of the database is restored to the Remote Geographic Node server.

Procedure

1. Log on to the active CCMM server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
3. Click **Backup Locations**.
4. Click **Create**.
5. From the **Drive Letter** list, select the network drive on which you want to store the CCMM database.
6. In the **UNC Path** box, type the location to store the backup, in the format `\\Computer Name\Backup Location`.

   This location must be a shared folder with correct permissions.

   Important:

   When Contact Center Multimedia is installed as a standalone server, do not use the same backup folder for your co-resident and multimedia ADMIN databases, as ADMIN databases stored in the same backup location overwrite each other.
7. In the **User Name** box, type the user name used to log on to the computer specified in the UNC Path box.

   The user name is in the format `Computer Name\Account Name`.
8. In the **Password** box, type the domain password.
9. Click **OK**.
10. In the left pane, click **Immediate Backup**.
11. In the **Media Type** section, select **Network Disk**.
12. In the **Applications** section, select **CCMM** and **ADMIN**.
13. From the **Backup Location** list, select the network drive on which to store the backup.
14. Click **OK**.

Restoring the database on the Remote Geographic Node server

Before you begin

- When CCMM is installed, the license type is NODAL. If you have a Corporate (CORP) license, this must be set on the Remote Geographic Node server, before the active server backup is restored on to the Remote Geographic Node machine.

Important:

Restore the CCMM database first and then the ADMIN database.

Important:

Restoring the ADMIN database can change configuration of Backup locations on the Remote Geographic Node Server, if the Active Server and Remote Geographic Node Server backup locations are different. After you restore the ADMIN database, close and reopen the Database and Maintenance utility.

About this task

Restore the database from the Active Server to the Remote Geographic Node Server to ensure the databases are consistent. The Database Maintenance utility can restore only one application's data at a time. Therefore restore the data for the CCMM and ADMIN databases.

You must restore the CCMM and ADMIN databases to the Remote Geographic Node Server. Restore the ADMIN database last.

Procedure

1. Log on to the Remote Geographic Node Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
3. In the **Database Maintenance** dialog box, in the left pane, click **Restore**.
4. In the right pane, under **Media Type**, select the media type on which the backup is restored.
5. If the backup file is on the network drive, in the **Backup Location** list, select the backup location.
6. Under **Application**, select the database to restore.
7. Under **Restore contents**, select **Data**.
8. Click **OK**.
9. Use the **Progress information** field to monitor the progress of the restoration.

10. Click **Exit** to close the Database Maintenance utility.

Configuring RGN CCMM General Administration

Before you begin

- Launch the RGN CCMM Dashboard and change the CCMA server name to be the RGN CCMA server name.
- Log on to the Contact Center Manager Administration application on the Remote Geographic Node server.

About this task

Configure the Remote Geographic Node (RGN) Contact Center Multimedia (CCMM) server to use local telephony and multimedia resources.

In a multimedia-enabled solution Agent Desktop client software is typically downloaded from a Contact Center Multimedia (CCMM) server. Agent Desktop then communicates with that Contact Center Multimedia server to handle e-mail based contacts. Agent Desktop communicates with a Communication Control Toolkit (CCT) server to handle voice contacts.

Important:

Changes to the RGN CCMM Server Settings may require a RGN CCMM server restart before they take effect.

Procedure

1. Under the **Launchpad**, select **Multimedia** from the drop down list.
2. In the left column, select **General Administration**.
3. Click **Server Settings**.
4. Change the **Contact Center Manager Server** to the IP address or name of the Remote Geographic Node CCMS server.
5. Change the **Contact Center License Server** to the IP address or name of the Remote Geographic Node License Manager server.
6. Change the **Contact Center Manager Administration** to the IP address or name of the Remote Geographic Node CCMA server.
7. Change the **Contact Center Multimedia Server** to the IP address or name of the Remote Geographic Node CCMM server.
8. Change the **Contact Center Multimedia Standby Server** box to not configured.
9. Change the **Communication Control Toolkit Server** to the IP address or name of the Remote Geographic Node CCT server.

10. Change the **Standby CCT Server** box to not configured.
11. Change the **Geographic Alternate CCT Server** box to not configured.
12. Configure **CC Web Stats**. If the Contact Center Web Statistics Server does not exist, click **New** to create one.
13. In the left column select **Email**.
14. Click **General Settings**.
15. Ensure that the Inbound URL is of the form `http://<RGNIPAddress>/inboundattachment`.
16. Ensure that the Outbound URL is of the form `http://<RGNIPAddress>/outboundattachment`.

Variable definitions

Name	Description
Contact Center Manager Server	Enter the IP address or name of the RGN CCMS server.
Contact Center Multimedia Server	Enter the IP address or name of the RGN CCMM server.
Contact Center License Server	Enter the IP address or name of the RGN LM server.
Contact Center Multimedia Standby Server	Not Configured.
Communication Control Toolkit Server	Enter the IP address or name of your RGN CCT server.
Standby CCT Server	Not Configured.
Geographic Alternate CCT Server	Not Configured.
CC Web Stats	The name of the optional Web Statistics server that agents and supervisors use to view real-time statistics for call handling, skillset data, and the state information on the Agent Desktop. This is typically the CCMS server.

Configuring the Remote Geographic Node Server

Before you begin

- The database from the Active server has been restored to the Remote Geographic Node server.

About this task

Configure the Remote Geographic Node CCMM server.

Procedure

1. Log on to the Remote Geographic Node Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. In the left pane, click **Server Mode**.
4. In the **Server Mode Configuration** section, select **Standby**.
5. Under **IP Configuration**, leave the **Managed IP** details blank.
6. Under **IP Configuration**, type the **Active Server details**, **CLAN** IP address.
7. Under **IP Configuration**, in the **Standby Server details** section, in the **CLAN** IP address box, type the IP address for the Remote Geographic Node Server.
8. Click **OK**.
   A system message box appears. You must stop the system before you save any information.
9. Click **OK**.

Variable definitions

Name	Description
Active Server details	Type the virtual Managed IP address that is used by the active CCMM server for campus resiliency. The CCMM Remote Geographic Node server monitors the Managed IP address of the campus CCMM site. If the Active CCMM server on the campus site fails, the Standby CCMM server assumes

Name	Description
	the managed IP address and continues processing. The CCMM Remote Geographic Node server monitors this campus Managed IP address and therefore continues shadowing.
Standby Server details	The IP address for the Remote Geographic Node Server.
Trusted IP address	Avaya recommends that you use the IP address of some part of your IT infrastructure, that is always available to respond to a ping request, as the Trusted IP address.

Starting the Active Server

About this task

Start the Active Server using the CC Applications tab in the High Availability utility. Starting the Active Server starts the system processes.

Procedure

1. Log on to the Active Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Tasks**.
4. Double-click **CC Applications**.
5. In the first box under **CC Applications**, select the system.
6. Click **Start**.
7. Click **OK**.

Starting shadowing on the Remote Geographic Node Server

About this task

Use the High Availability utility to start shadowing on the Remote Geographic Node Server.

Important:

You must backup the Active server database, restore it onto the Remote Geographic Node server, and enable shadowing within 24 hours. If the difference in time between the Active and Remote Geographic Node server database content is greater than 24 hours, then database shadowing does not work. If shadowing is stopped for more than 24 hours then you must backup the Active server database and restore it onto the Remote Geographic Node server before re-enabling shadowing. Ensure that the system clock time on the Active and Remote Geographic Node servers are synchronized.

Procedure

1. Log on to the Contact Center Multimedia Remote Geographic Node server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.
4. Beside **Control**, select **Shadowing**.
5. Click **Start**.

Verifying shadowing is running on the Active Server

About this task

The system information tab of the High Availability utility displays system information regarding the Active and the Remote Geographic Node servers. The dialog box displays the following information categories:

- Computer name and operating system version
- Server mode
- Server configuration type
- Port information
- Remote server connection status

- Remote server port information
- License information
- Databases shadowed
- Time of last record shadowed
- Database namespaces
- Local and remote information on system status, switchover, shadowing, and network.
- CC Application install information
- Database space and journaling information
- Database processes information

Use this procedure to verify the settings.

Procedure

1. Log on to the active CCMM server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **High Availability**.
3. Expand **Configuration**.
4. Select **System**.
5. Select **Get System Configuration**.
   The most recent system information appears.
6. Under the **Shadowing** section, view the time of the most recent shadowed record.

   Ensure it has an up-to-date time, which corresponds with when shadowing was started.

Chapter 28: Communication Control Toolkit commissioning for Knowledge Worker

Use the procedures in this section for commissioning the Communication Control Toolkit software in your knowledge worker or direct-connect environment. A knowledge worker configuration supports telephony service routing directly with the Avaya Communication Server 1000 PABX.

Prerequisites to CCT commissioning for Knowledge Worker

- Read *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Complete *Avaya Aura® Contact Center Installation Checklist* (NN44400-310).
- Install all of the components required for the Communication Control Toolkit software for your network configuration, including the updates. For more information, see *Avaya Aura® Contact Center Installation* (NN44400-311).
- Ensure the appropriate PABX is installed and configured for your system.
- Install Communication Control Toolkit and all current updates.
- Install License Manager software and all current updates.

Communication Control Toolkit commissioning for Knowledge Worker procedures

About this task

This task flow shows you the sequence of procedures you perform to configure Communication Control Toolkit in a Knowledge Worker or direct-connect environment.

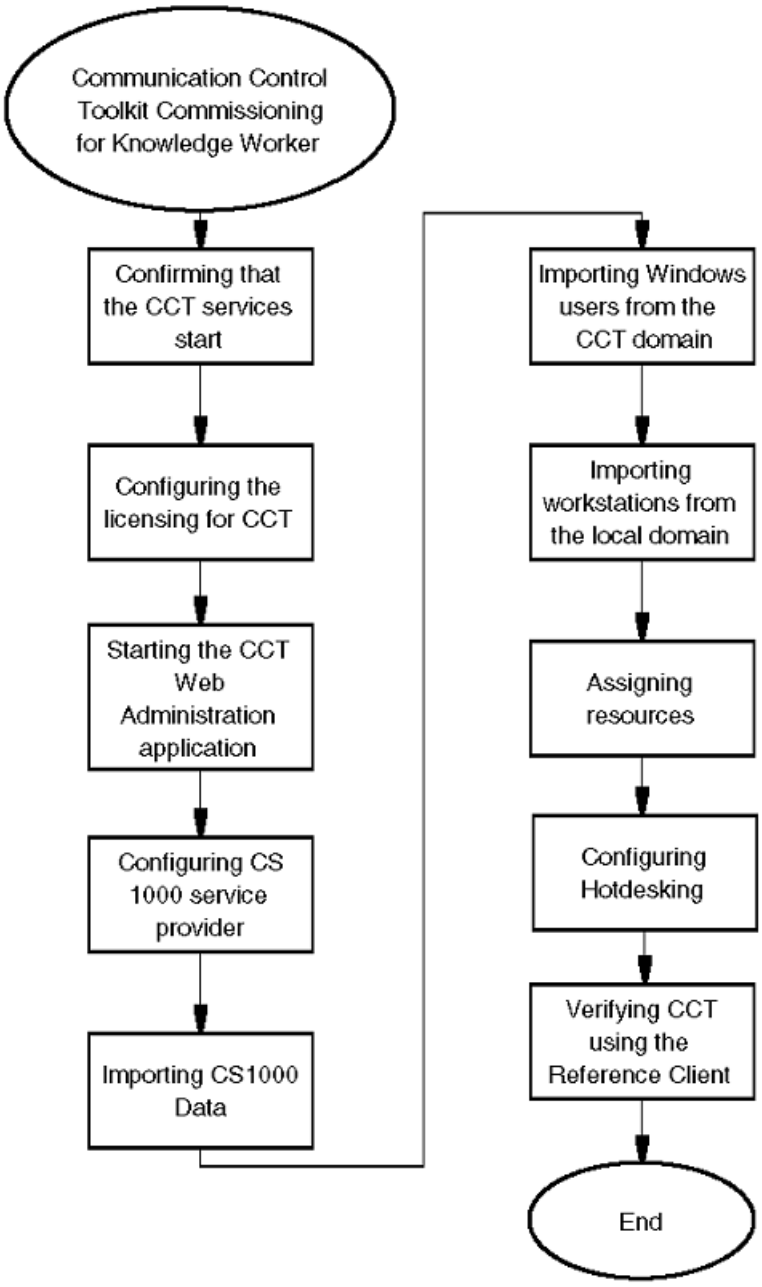


Figure 57: Communication Control Toolkit commissioning for Knowledge Worker procedures

Confirming that the CCT services start

About this task

Confirm that the CCT services start so you can configure the Communication Control Toolkit database.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**.
2. Select the **CCT** tab.
3. Confirm that the Communication Control Toolkit services are running.
4. If a Communication Control Toolkit service is not running, re-start CCT services.
5. Close the **SCMU** utility.

Procedure job aid

The following Communication Control Toolkit services must start:

- Caché Service
- NCCT SMON
- NCCT Logging Service
- ACD Proxy Service
- Telephony
- NCCT Data Access Layer
- NCCT TAPI Connector
- NCCT Server
- NCCT OI Service
- Contact Center Tomcat Instance

Configuring the licensing for CCT

Before you begin

- Contact Center License Manager is installed.

About this task

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

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

Procedure

1. Log on to the Communication Control Toolkit server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
3. Expand Communication Control Toolkit.
4. Expand **Server Configuration**.
5. Click **License Configuration**.
6. In the right pane, under **Primary License Manager Server**, in the **IP Address** box, type the IP address for the server on which the License Manager is installed.
7. Under **Secondary License Manager Server**, in the **IP Address** box, type the IP Address for the server on which the secondary License Manager is installed.

   Important:

   The Secondary License Manager Server IP Address section is 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**.

Variable definitions

Name	Description
License Type	The type of license for the License Manager. Nodal—The license applies to only one installation of CCMS. You cannot configure the Secondary License Manager for a Nodal license. Corporate—The license applies to a collection of Contact Center Manager Servers. Secondary License Manager is 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.
Secondary License Manager Server IP Address	The optional IP address of the server on which the backup License Manager application is installed.

Starting the CCT Web Administration application

About this task

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.

Procedure

1. Open Internet Explorer.
2. Type the URL http://<CCT IP address>:8081/WebAdmin/.

   The CCT port number, 8081, is the default port number. If you are using a different port number for security reasons, ensure that you use the configured port number for your system.

Configuring the Avaya Communication Server 1000 service provider

Before you begin

- Understand the server provider details for the switch.

About this task

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 Avaya Communication Server 1000 service provider details.

Procedure

1. Start Communication Control Toolkit Web Administration.
2. In the resource menu list, select **Providers**.
   The details of the providers are displayed.
3. From the list of providers, select **Passive**.
4. In the **Basic Provider Information** section, in the **Passive Name** box, type the Provider name.

   Important:

   The provider name must be Passive.
5. In the **IP Address** box, type the IP address of the provider.
6. In the **Port** box, type the port number.
7. In the **Provider Configuration** section, select the **Transport** type, **TCP**.
8. In the **Customer Number,** type the customer number.
9. From the **CS1000 Software Release** list, select the software release of your Avaya Communication Server 1000.
10. In the **Call Data Life Span (minutes)** box, type the required value in minutes.
11. Select or clear the **Disable Copy of Data to Consult Call** check box.
12. In the **CS1000 Home location Code (HLOC)** box, type the HLOC value.
13. In the **Network IVR Port** box, type the port value.
14. In the **Initialization Timeout (seconds)** box, type the **Initialization timeout** setting in seconds.
15. In the **Command Timeout (seconds)** box, type the **Command** timeout setting in seconds.

16. Select **Save**.

Variable definitions

Name	Description
Provider Name	Name of the Provider, Passive.
IP Address	In a Knowledge Worker environment, the IP address of the Avaya Communication Server 1000.
Port	In a Knowledge Worker environment, the port value is 8888.
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.
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 Avaya 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.

Name	Description
	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.

Importing Avaya Communication Server 1000 Data

Before you begin

- Connect a COM cable from a server (not the Communication Control Toolkit server) or workstation to the switch.
- Know the user ID and password to log on to the Avaya Communication Server 1000.
- Apply all Avaya Communication Server 1000 patches, specifically patch MPLR26704. Patch MPLR26704 significantly reduces the time to import address and terminal information into the text file. Only information that is relevant to Communication Control Toolkit is imported.
- Only PABX keys that are AST and IAPG enabled are imported.

About this task

You can use the CCT Import CS 1000 Data tool to perform either of the following activities:

- 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”.

You can convert the text file to an XML file to test the data import facility without modifying the database contents; or, you can 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 you import the Avaya Communication Server 1000 data to CCT, you must first retrieve the data from the switch. To retrieve the data, create a switch configuration text file to capture the Avaya Communication Server 1000 data required to configure Communication Control Toolkit.

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

Procedure

1. Open a text editor on the server where the Hyperterminal is installed.

2. Create a new text file called **download.txt**.
3. Click **Start** > **All Programs** > **Accessories** > **Communications** > **HyperTerminal** to connect to the Avaya Communication Server 1000.
4. Type a name for the connection.
5. Click **OK**.
6. On the **Connect To** dialog box, in the **Connect using** list, select COM1 or the COM port connected to the Avaya Communication Server 1000 switch.
7. Click **OK**.
8. In the **COM properties** dialog box, verify the data is correct or make necessary changes.
9. Click **OK**.
10. From the **Transfer** menu, select **Capture Text**.
11. In the **Capture Text** dialog box, type the location and name of the text capture file in the **File** box, for example, type the location and name of the **download.txt** file created in step 2.
12. Click **OK**.
13. At the prompt, type **logi admin1** to log on to the switch.
14. Type your user ID and password for the switch.
15. If the prompt does not appear, continue to press **Enter** until the prompt appears.
16. Browse to the download.txt file, and then click **Start**.
17. Type these commands at the following prompts:

    ```
    >LD 20
    REQ: PRT
    TN: TNB
    TN: Press enter
    CDEN: Press enter
    CUST: 0 (or the customer number)
    DATE: Press enter
    PAGE: ON
    DES: Press enter
    ```

    Downloading information from the Avaya Communication Server 1000 overlay can take a several minutes.
18. To return to the prompt, enter ******** (Shift + 8888).
19. Press **Enter**.
20. Type these commands at the following prompts:

    ```
    >LD 23
    REQ: PRT
    TYPE: CDN
    CUST: 0 (or the customer number)
    CDN: Press enter
    ```

    The information is downloaded from the overlays.

21. Type **logo**.
22. Press **Enter**.
23. Copy the download.txt to the Communication Control Toolkit server.
24. Log on to the Communication Control Toolkit server.
25. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
26. Expand **Communication Control Toolkit**.
27. Expand **Bulk Provisioning**.
28. Select **Import CS 1000 Data**.
29. Select **Passive** for the Avaya Communication Server 1000 Provider.
30. Select **Input File**. This opens a file explorer to select the Avaya Communication Server 1000 data capture file you copied in step 23 on page 460.
31. Select the Avaya Communication Server 1000 data capture file, click **Open**. A default path and file name appears 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, select **Convert/Import**. A progress bar in the Status area indicates the progress made by the tool in three phases:
    - Conversion of the data capture file
    - Generation of the output file
    - Import of the data into the database
34. The status area displays data imported and the conversion results, including the number of TNs, DNs, and CDNs found. If applicable, a list of errors are also displayed. This list includes line numbers where the errors were discovered in the supplied data capture file.

    Important:

    An error dialog shows errors in the conversion step. The error dialog appears prior to beginning the automatic import. The user can choose to cancel the import step or proceed.

Importing Windows users from the CCT domain

Before you begin

- Ensure that the local administrator has user access for the contact center domain. The local administrator needs domain access to import domain users using the CCT Snap-in Console.

About this task

Import windows users from the contact center domain server to Communication Control Toolkit using the Import Windows Users tool. After the users are imported in the CCT Snap-in Console, you can configure the resources in the CCT Web Administration client.

Procedure

1. Log on to the Communication Control Toolkit server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
3. Expand Communication Control Toolkit.
4. Expand **Bulk Provisioning**.
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**, a **First Name**, or a **Last Name**.
8. In the **Begins With** box, type the text to use in a search for Windows Users.
9. In the **Actions Pane** on the right, select **Search For Users.**
10. In the **Search Results** box, select the Windows users to import.

    To select multiple users, press the **Ctrl** key while you select each user. To select all Windows users, click **Add All**.
11. Click **Add**.
12. In the Actions pane, select **Import Selected Users**.

Variable definitions

Name	Description
Search Type	The criteria for selecting a small group of Windows user accounts to import to the Communication Control Toolkit. You can choose one of the following options: • Find All Users—find all Windows user accounts on the CCT server. • Login Name—find all Windows user accounts where the user name or logon ID matches or contains the value in the Begins With box. • First Name—find all Windows user accounts where the first name matches or contains the value in the Begins With box. • Last Name—find all Windows user accounts where the last name matches or contains the value in the Begins With box.
Begins With	A string of characters to match the beginning of the text with in the search for the selected Search Type.

Importing workstations from the domain

Before you begin

- A local administrator must have access to the contact center domain to import domain resources to CCT. Domain resources that can be imported are domain users and domain workstations. Ensure the local administrator has access to the contact center domain.

About this task

All Contact Center applications are in a contact center domain. Import workstations from the contact center domain to the Communication Control Toolkit server using the Import Workstations tool.

Procedure

1. Log on to the Communication Control Toolkit server.

2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
3. Expand **Communication Control Toolkit**.
4. Click **Import Work Stations**.
5. From the **Search Type** list, select **All WorkStations**.
6. From the **Available Work Stations** list, select the workstations to import.
7. Click **Add**.
8. Click **OK**.

Assigning resources in Knowledge Worker

About this task

Resources in CCT are users, terminals, addresses, and workstations. To enable CCT to work 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

1. Launch the **CCT Web Administration client**.
2. Click the resource type.
3. Click the single resource to configure.
4. Select one of the Resource Assignments to assign to this resource.
5. 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.
6. Click **the Right Arrow** to move the selected resource and resource groups to the **Assigned Resources** column.
7. Click **Save**.

Example of assigning resources

About this task

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.

Procedure

1. Launch the **CCT Web Administration** client.
2. Select **Groups**.
3. Select **Terminal Groups**.
4. Select the hotdesking_terminals terminal group.
5. Select the all terminals in the **Available Resources** column.
   Click each resource to select more than one resource.
6. Click **the Right Arrow** to move the selected terminals to the **Assigned Resources** column.
7. Click **Save**.

Configuring Hotdesking (Agent Roaming)

Before you begin

- 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.

About this task

In a contact center an agent may not have a fixed desk and phone. An agent may pick a desk that is not being used and log into the phone and workstation. An agent must be able to log on to any phone and workstation in this environment.

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.

Procedure

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.

   Important:

   A terminal can only be assigned to one workstation.

Verifying CCT using the Reference Client

Before you begin

- Import the resources from the external sources to the Communication Control Toolkit Console. See the following sections:
  - Importing Avaya Communication Server 1000 Data on page 458
  - Importing Windows users from the CCT domain on page 461
  - Importing workstations from the domain on page 462
- Assign the required resources in the Communication Control Toolkit Console. See Assigning resources on page 463.
- Create a Windows user for testing.

About this task

Verify Communication Control Toolkit by using the Reference Client to ensure that all resources are available and accessible. The Reference Client is only an installation testing tool and not to be deployed for production contact center use.

You can use several user IDs to log on to the Reference Client to make calls between them to test connections, transfers, and other call functions.

Procedure

1. Log on to the Communication Control Toolkit server with the Local Administrator user ID and password.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **Ref Client**.
3. In the **Server Settings** dialog box, click **OK**.
4. From the **Session** menu, choose **Connect**.
5. In the **User Credentials** dialog box, select either the **Current Windows User** or specify a **User ID**, **Domain** and **Password**.
6. Click **OK**.
7. In the **Available Devices** box, select the address you want to use for the test call.
8. Enter the Destination Address in the text box to the right of the Originate button.
9. Click **Originate**. The destination address shows a Local State of Ringing in the Reference Client
10. Select the Ringing Address on the Reference Client, and click **Answer**.
11. Release the call.

Chapter 29: Integrated Reporting commissioning

This section describes how to commission Integrated Reporting.

Contact Center Manager Server (CCMS) has an integrated reporting capability for Multimedia (CCMM) and Avaya Media Server statistics.

You can configure CCMS to collect and store Avaya Media Server and CCMM statistical contact data in the CCMS database. You must select the CCMS Contact Summary Reporting (CSR) feature to enable Integrated Reporting.

The Avaya Media Server database location, username and password may be entered in the CCMS Database Maintenance utility, allowing CCMS to collect Avaya Media Server statistical data every 15 minutes and store it in the CCMS database.

The Contact Center Multimedia database location, username and password may be entered in the CCMS Database Maintenance utility, allowing CCMS to access CCMM statistical data directly without storing it in the CCMS database.

For front-end IVR scenarios, Avaya Media Server assigns a unique number to each call. Avaya Media Server passes this unique call number to the CCMS Open Networking web service, as the call is transferred to the CCMS. The CCMS then uses this unique call number to match the Avaya Media Server part of the call with the CCMS part of the same call and generate meaningful call flow statistics. The CCMS Open Networking Web Service must be enabled for this procedure to work. For Avaya Media Server treatment scenarios, the call arrives first on CCMS, which assigns it a unique number. When the call is treated by Avaya Media Server, this unique number is extracted by the Avaya Media Server application using CTI, and stored in the reporting data for this part of the call. The Open Networking Web service is not required for the Avaya Media Server treatment scenario. Contact Summary Reporting must be enabled on the CCMS to collect these CSR statistics.

The Avaya Media Server uses a Landing Pad, a CDN controlled by the CCMS, to transfer the call to the Contact Center.

Prerequisites for Integrated Reporting commissioning

- Read the *Avaya Aura® Contact Center Planning and Engineering* (NN44400-210).
- Complete the *Avaya Aura® Contact Center Installation Checklist* (NN44400-310).
- Install the Contact Center Manager Server software.

- Install the other Avaya Aura® Contact Center components on your server.
- The system clock time must be the same on both the CCMS and Avaya Media Server server. The time zones can be different, if for example the Avaya Media Server server is in Eastern time zone and CCMS is in the GMT time zone, the system clock time must be the same on both servers. CCMS already obtains the time from the Avaya Communication Server 1000, therefore all Contact Center servers have the same clock. To ensure that the system clock time on the CCMS and the Avaya Media Server servers are synchronized configure the system so that they both obtain their times from the same external clock source. This is achieved as follows:
  - Configure the Avaya Media Server Network Time Protocol (NTP) service as a client of an external time source clock.
  - Configure the Avaya Communication Server 1000 time service as a client of the same external time source clock as used for Avaya Media Server.
- Contact Center collects data from only one Avaya Media Server. If the Contact Center interacts with multiple Avaya Media Server servers on a Cluster, create the replication account for Integrated Reporting on the Active or Secondary with appropriate Session Detail Record (SDR) replication settings. Integrated Reporting supports only one cluster. If more than one cluster is configured, only one of them can be designated as the Integrated Reporting cluster.

Commissioning Integrated Reporting

About this task

This task flow shows you the sequence of procedures you perform to configure Integrated Reporting.

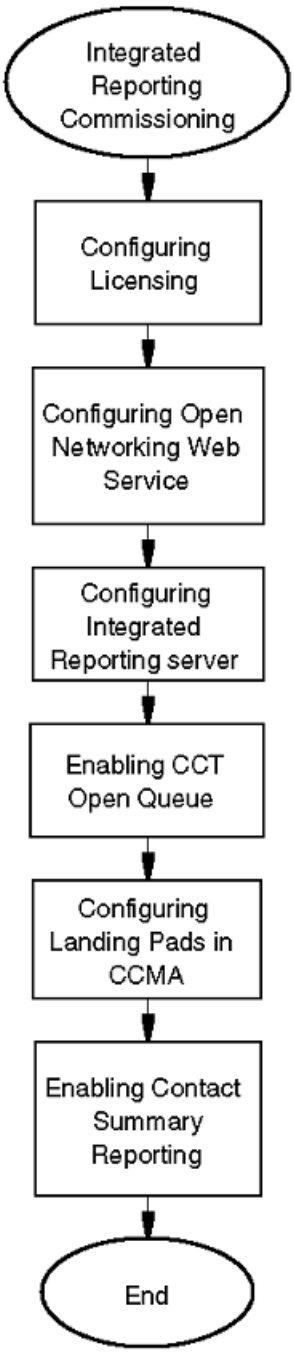


Figure 58: Integrated Reporting commissioning procedures

Job aid: Timing

The estimated time to commission Integrated Reporting is 1 hour.

Configuring licensing

Before you begin

- Install the Open Queue feature.
- The Universal Networking feature is available with an Enterprise license.

Important:

You must restart your server at the end of this procedure.

About this task

Use this procedure to configure licensing to enable the Open Networking feature.

Procedure

1. Log on to the Contact Center Manager Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
3. Click the **Licensing** tab.
4. From the **CCMS Optional Packages** list, select **Networking**, **Universal Networking**.
5. Select **Open Queue**. Enable this option even if Open Queue is not otherwise being used.
6. Select **Open Interfaces Universal Networking**.
7. Click **OK**.
8. Click **Yes** to restart the server.

Procedure job aid

After you restart Contact Center Manager Server, Open Queue is enabled.

Configuring Open Networking Web service

Before you begin

- Know how to stop and restart the core CCMS services.
- Ensure that a valid SOA license is available.
- The Open Networking Web service is available only if the customer purchased the Universal Networking feature, and selected the enable SOA option on the CCMS order.
- If enabling TLS, understand Certificate Authorities, certificate signing requests, and certificates.
- A Certificate Authority is also required to generate the certificates.

Important:

You must restart your server after you perform this procedure.

About this task

Use this procedure to configure the Open Networking Web service.

Procedure

1. Log on to the Contact Center Manager Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
3. In the left pane of the Server Configuration console, click **WS Open Interfaces**.
4. Select the **SOA Enabled** check box.
5. Ensure the **Host** contains the host name of the server.
6. In **Ports**, type an available port number for which the services are available for access.
7. In the **Session Timeout** box, select the value of the timeout duration in minutes.
8. To publish services under TLS (HTTPS), select the **TLS Encryption** check box. To publish services under HTTP, clear the **TLS Encryption** check box.
9. Click **Apply All**.
10. Click **OK**.
11. Select **Exit** to save your changes.
12. Stop and restart the core Contact Center Manager Server services.

Variable definitions

Name	Description
Host	The host name of the server, not the IP address.
Ports	The port number on which the OpenQueue and OpenNetwork Interfaces are published. This port and the following three consecutive port numbers are used to access the Web services from the external applications. All four port numbers must be available.
Session Timeout	The time in minutes that a session is valid after a user logs on. The session times out if it is inactive for the specified duration. The default is 120 minutes.
TLS Encryption	To publish services under TLS (HTTPS), mark the TLS Encryption check box. To publish services under HTTP, clear the TLS Encryption check box.

Procedure job aid

Once enabled, the WSDL for the Open Networking web service is available at: `http://<CCMS HostName>:9080/SOAOI/services/OpenNetworking?wsdl`

Configuring Integrated Reporting Server

Before you begin

- If integrating CCMS with Avaya Media Server, the Avaya Media Server database replication userID account and password must be setup on the Avaya Media Server using Element Manager. This account and password are needed by CCMS to access the Avaya Media Server reporting server to collect statistics for Integrated Reporting. This account is set up using the Avaya Media Server Element Manager under - Replication Account.
- Contact Center collects data from only one Avaya Media Server. If the Contact Center interacts with multiple Avaya Media Servers on a Cluster, this replication account must be created on the Active or Secondary with appropriate SDR replication settings.

Integrated Reporting supports only one cluster. If there is more than one cluster, only one of them can be designated as the Integrated Reporting cluster.

- If integrating with CCMM, use the CCMM mmReport account and its password. These are set up during the CCMM installation.

About this task

Add Avaya Media Server and Contact Center Multimedia (CCMM) as Integrated Reporting Servers using the CCMS Database Maintenance Utility. The CCMS Database Maintenance Utility - Integrated Reporting Server supports one CCMM server and one Avaya Media Server.

Use the CCMS Database Maintenance utility to configure one Avaya Media Server and one CCMM server to enable integrated reporting for Avaya Media Server Contact Summary Report (CSR) statistics and MM CSR statistics.

Procedure

1. Log on to the Contact Center Manager Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Database Utilities** > **Database Maintenance**.
3. In the Database Maintenance dialog box, in the left pane, click **Integrated Reporting Server**.
4. In the right pane, click **Create** to add a new row to the Server table.
5. From the **Type** list, select the type **ICP** or **MULTIMEDIA** from the list. This automatically populates the **Port** and**Database Name** columns.
6. In the **Display Name** box, type the Avaya Media Server name, or the CCMM server as it appears in future reports.
7. In the **IP** box, type the IP address of the Avaya Media Server or CCMM server.
8. In the **Username** box, type the Avaya Media Server database replication account username, or the CCMM mmReport user name.
9. In the **Password** box, type the Avaya Media Server database replication account password, or the CCMM mmReport password.
10. Click **OK**.
11. Click **Exit**.

Variable definitions

Name	Description
Type	ICP or MULTIMEDIA, as appropriate. If the server type is Avaya Media Server select the ICP option.
Display Name	The Avaya Media Server or CCMM server name as it appears in future reports.
IP	The IP address of the Avaya Media Server or CCMM server.
Port	Automatically filled in.
Database Name	Automatically filled in.
Username	The Avaya Media Server replication account user name. Or the CCMM mmReport account name.
Password	The Avaya Media Server replication account password Or the CCMM mmReport account password.

Enabling Communication Control Toolkit Open Queue

Before you begin

- Open Queue must be enabled on the CCMS.
- Know how to stop and restart the core Communication Control Toolkit services.

About this task

Enable Open Queue functionality on stand alone Communication Control Toolkit (CCT). If CCT is co-resident with CCMS, enable Open Queue on CCMS, see Enabling Open Queue on page 35.

Procedure

1. Log on to the Communication Control Toolkit server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
3. In the left pane of the CCT console, expand **Communication Control Toolkit**.
4. Expand **Server Configuration**.

5. Select **Deployment Type**.
6. In the **Deployment Type** dialog box, select your deployment option for 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 core Communication Control Toolkit services.

Configuring landing pads

Before you begin

- The selected CDN must be configured on the switch.

About this task

Use this procedure to configure Landing Pads using CCMA.

Avaya recommends that you configure multiple Landing Pads to ensure proper capacity and scalability. The Open Networking Web service distributes load across all configured Landing Pads.

Although you can configure both CDNs and DNISs as Landing Pads, the Integrated Reporting feature is available when you use CDN Landing Pads only. For more information about Landing Pads, see *Avaya Aura® Contact Center Server Administration* (NN44400-610).

For more information on configuring Landing Pads see *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

Procedure

1. Log on to Contact Center Manager Administration.
2. On the CCMA web page, select **Configuration**.
3. In the left pane, double-click the Contact Center Manager Server on which to add the Landing Pad CDN (Route Point).
4. Select the CDNs (Route Points) folder.
5. In the **CDNs (Route Points)** window, select the **Landing Pads** tab.
6. In **Name** box, type a name for the CDN (Route Point) Landing Pad.
7. In the **Number** box, type the number for the CDN (Route Point) Landing Pad. This number must match the number configured on the switch.

8. For SIP Contact Centers, you must configure the Landing Pad URI. In the **URI** box, type the value for the Universal Resource Indicator (URI) of the CDN (Route Point) on the SIP server.
9. Click any other row in the grid to add the CDN (Route Point) Landing Pad. Not Acquired appears in the Status column.
10. Select the **Acquired** check box for the CDN (Route Point) Landing Pad.
11. Click any other row of the table to acquire the CDN (Route Point) Landing Pad.
12. Click **Refresh Status** to view the current status.

Variable definitions

Name	Description
Name	The name of the CDN (Route Point) as you want it to appear in reports. Valid value: 30-character maximum (no special characters)
Number	The number assigned to the CDN (Route Point). The number passed to the switch in requests to acquire or deacquire the CDN (Route Point). This number must match the number configured at the switch. **Important:** You cannot change a saved CDN (Route Point) number. You must delete the CDN and then recreate it. Valid values: 7-digit maximum.
URI	URI box (only present for SIP connected contact centers). The Universal Resource Identifier (URI) of the CDN (Route Point) on the Avaya Media Server. The URI must equate to the fully qualified SIP address for the CDN (Route Point). Valid values: maximum 255 characters, including numbers, English characters, forward slash (/), backslash (\), question mark (?), ampersand (&), period (.), at symbol (@), underscore (_) and hyphen (-).

Name	Description
	This is mandatory. You cannot modify the URI of a saved CDN (Route Point). The URI must be unique to URIs currently assigned to other CDNs, DNISs, or agents.
Acquired	**Important:** You must configure the CDN (Route Point) on the switch and add it on Contact Center Manager Server before you can acquire it. Select the Acquired check box to acquire or deacquire the CDN (Route Point) and then click Refresh Status to refresh the Status column. If the acquisition is successful, Acquired appears in the Status column. When you successfully deacquire the CDN (Route Point), Not Acquired appears in the Status column.
Status	The Status column displays the acquisition status of the CDN (Route Point) or Open Queue CDN (Route Point).

Enabling Contact Summary Reporting

About this task

Contact Summary Reporting (CSR) must be enabled on the CCMS server for the Integrated Reporting to be enabled. Integrated Reporting then returns the statistical data for Avaya Media Server CSR and CCMM CSR.

You must enable the Contact Summary Reporting using CCMA – Configuration component under Historical Statistics node.

For more information, see Configuring Historical statistics in *Avaya Aura® Contact Center Manager Administration – Client Administration* (NN44400-611).

Procedure

1. Log in to Contact Center Manager Administration.
2. On the CCMA web page, select **Configuration**.
3. In the left pane, double-click the server on which to configure Historical Statistics.
4. Select the **Historical Statistics** folder.
5. In the right-pane, select the **Collect the following statistics** table.

6. For each statistic type, in the **Collect** column, select the check box beside the statistics to collect, or clear the check box beside the statistics not to collect.
7. In the **Collect the following statistics** table, select the **Contact Summary** check box.
8. Scroll down and select the **Duration** table.
9. For each type of statistic, enter the amount of time the statistic is stored on the server.
10. In the **Duration** table, enter one or more days as appropriate for **Contact Summary (days)**.
11. Click **Submit** to save your changes.

Chapter 30: Contact Center Manager Server Web service configuration

A series of SOAP-based Open Interfaces is provided to third-party software structures so that you can enable communications for your applications based on the SOA architecture.

The Open Queue Open Interface provides existing OpenQ functions to third-party applications using a Web service. In a controlled fashion, third-party applications can add and remove contacts of a specific type in Avaya Aura® Contact Center.

The Open Networking Open Interface enables a third-party application to transfer a call between nodes in a network along with any data associated with the call. The third-party applications can reserve a Landing Pad on the target node to enable the call to be transferred with data attached. The Web services also provide the functionality to cancel the reservation of a Landing Pad to free it for other calls transferred across the network.

The open interface applications are optional.

For more details, see the SDK documentation.

Generating a Certificate Signing Request

About this task

Generate a Certificate Signing Request (CSR) to configure certificates and enable the Web services over the Transport Layer Security.

Procedure

1. Log on to the Contact Center Manager Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
3. In the left pane of the Server Configuration console, click **WS Open Interfaces**.
4. Select the **TLS Encryption** check box.
5. Ensure the **Host** box contains the host name of the server.
6. In the **Password** box, type a password that contains at least six characters.
7. Click **Apply All**.

The CSR appears in the CSR box. Use the CSR file to apply to a Certificate Authority (CA) to buy a certificate and import the certificate to the service using the configuration application.

8. Click **OK**.

Variable definitions

Name	Description
TLS (Transport Layer Security)	Protocol that allows secure communication between applications across a network.

Procedure job aid

Certificate Authorities (CA) include the following components:

- Verisign
- Thawte
- Create your own

Importing the CSR-Related Certificates

Before you begin

- Ensure you generate a CSR certificate. For more information, see Generating a Certificate Signing Request on page 479.
- Ensure you apply to a Certificate Authority (CA) for a certificate.

About this task

Import the CSR-Related Certificates to the SOA configuration after you receive the certificates to enable services over the Transport Layer Security.

Procedure

1. Log on to the Contact Center Manager Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
3. In the left pane of the Server Configuration console, click **WS Open Interfaces**.

4. In the **Generate Certificate Signing Request Password** box, type a password.
5. In the **Alias** box, type an alias to identify the CA certificate, such as SomeCAPublicCert1.
6. In the **Trusted Certificate Authority CA Cert** box, click **Browse**, and then select the CA public certificate.
7. In the **CSR Response Certificate CSR Cert** box, click **Browse**, and then select the certificate.
8. Click **Apply All**.
9. Click **OK**.

Configuring SOA OpenQueue and OpenNetworking Web Services

Before you begin

- Know how to stop and restart the core CCMS services.
- Install and commission Contact Center Manager Server. See *Avaya Aura® Contact Center Installation* (NN44400-311) and *Avaya Aura® Contact Center Commissioning* (NN44400-312).
- Ensure that the Contact Center License Manager is licensed to provide SOA OpenQueue and OpenNetworking Web Services.
- If you enable TLS, understand Certificate Authorities, certificate signing requests, and certificates. A Certificate Authority is also required to generate the certificates. Configure the SOA Configuration of Certificates using the procedure in Generating a Certificate Signing Request on page 479.
- Ensure OpenQ and OpenNetworking Web Services and the CCT Web Services do not use the same port on the server. Change the OpenQ and OpenNetworking services port value from 9080 to 9070 in the Web services section of server configuration.

About this task

Configure and enable the SOA OpenQueue and OpenNetworking Web Services to configure other applications that can add contacts to the open queue for routing, remove contacts from the open queue, and move contacts between nodes in a network.

Procedure

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

3. In the left pane of the Server Configuration console, click **WS Open Interfaces**.
4. Select the **SOA ENABLED** check box.
5. Ensure the **Host** box contains the host name of the server.
6. In the **Ports** box, type an available port number for which the services are available for access.
7. In the **Session Timeout** box, select the value of the timeout duration in minutes.
8. To publish services under TLS (HTTPS), select the **TLS Encryption** check box. To publish services under HTTP, clear the **TLS Encryption** check box.
9. In the **User Password** box, type the new password for the OpenWsUser account.
10. Click **Apply All**.
11. Click **OK**.
12. Stop and restart the core Contact Center Manager Server services.
13. Verify that the services are available by viewing the following on the host: *http://localhost:9090*.

Variable definitions

Name	Description
Host	The host name of the server, not the IP address.
Ports	The port number on which the OpenQueue and OpenNetwork Interfaces are published. This port and the following three consecutive port numbers are used to access the Web services from the external applications. All four port numbers must be available.
Session Timeout	The time in minutes that a session is valid after a user logs on. The session times out if it is inactive for the specified duration. The default is 120 minutes.
TLS Encryption	To publish services under TLS (HTTPS), select the TLS Encryption check box. To publish services under HTTP, clear the TLS Encryption check box.

Removing Certificate Configuration

Before you begin

- Clear the TLS Security check box.
- Ensure the certificates are configured. For more information, see Generating a Certificate Signing Request on page 479.

About this task

Remove certificate configuration to delete all imported certificates and any outstanding CSR files.

Procedure

1. Log on to the Contact Center Manager Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Manager Server** > **Server Configuration**.
3. In the left pane of the Server Configuration console, click **WS Open Interfaces**.
4. Select the **SOA Enabled** check box.
5. Select the **Remove Certificates** check box.
6. Click **Apply All**, and then **OK**.
7. In the confirmation dialog box, click **Yes**.
8. Click **OK**.

Chapter 31: Communication Control Toolkit Web service configuration

A series of SOAP-based Open Interfaces is provided to third-party software structures so that you can enable communications for your applications based on the SOA architecture.

The CCT Open Interfaces is a development environment that offers functionality similar to the CCT SDK but with the flexibility to choose your own development environment.

You can use these services to re-create Agent tools within your own applications or to access call control functionality for Avaya Aura® Contact Center from any business process.

The open interface applications are optional. For more details, see the SDK documentation.

Configuring SIP Call Recording

About this task

Configure the SIP Call Recording user account. This SIP Call Recording user account is a special user that is only used by the Call Recording server to connect to Communication Control Toolkit, and only using the OI interface.

Avaya recommend that the SIP Call Recording user account is a Windows domain user account, although no restriction is in place to prevent the selection of a local Windows Security Account Manager (SAM) account.

Procedure

1. Log on to the Communication Control Toolkit server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
3. In the left pane of the CCT console, Expand **Communication Control Toolkit**.
4. Expand **Server Configuration**.
5. Select **CCT Web Services**.
6. Select the **Enable CCT Web Services** check box in the right pane.
7. Under **SOA Configuration**, select the **Enable SIP Call Recording** check box.
8. Click **Browse Users**.

9. On the **Browse Users** dialog, in the **Location** list, select the location of the Windows account you plan to use as the SIP Call Recording user account.
10. In the Search Type list, select **All Users**.
11. Click **Search**.
12. From the list of users, select the user that you plan to use as the SIP Call Recording user account.
13. Click **OK**.

Generating a Certificate Signing Request

About this task

Generate a Certificate Signing Request (CSR) to configure certificates and enable services over the Transport Security Layer (TLS).

An application can use CSR to apply to a Certificate Authority (CA) for a certificate. The host name and password is used to generate the CSR. The password is saved in an encrypted format.

After the CSR file is generated and it is available to present to a Certificate Authority to obtain a corresponding certificate.

Procedure

1. Log on to the Communication Control Toolkit server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
3. In the left pane of the CCT console, Expand **Communication Control Toolkit**.
4. Expand **Server Configuration**.
5. Select **CCT Web Services**.
6. Select the **Enable CCT Web Services** check box in the right pane.
7. Select the **TLS Security** check box.
8. Ensure the **Host Name** box contains the host name of the server.
9. Click **Generate CSR**.
10. In the **Location** box, type the location of the company.
11. In the **Company Name** box, type the name of your company.
12. In the **Password** box, type a password that contains at least six characters.
13. Click **Generate**.

14. Click **OK**.

Important:

After you generate a CSR, import Trusted Certificate Authority (CA) for a certificate and import CSR Response Certificate then Apply Changes. These three steps are required to enable services over the TLS.

Variable definitions

Name	Description
TLS (Transport Layer Security)	Protocol for secure communication between applications across a network.

Importing CSR-related Certificates

Before you begin

- Ensure you generate a CSR certificate. For more information, see Generating a Certificate Signing Request on page 486.
- Ensure you apply to a Certificate Authority (CA) for a certificate.

About this task

After you receive the certificate, import the CSR-related certificates to the SOA configuration to enable services over the TLS.

Procedure

1. Log on to the Communication Control Toolkit.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
3. In the left pane of the CCT console, expand **Communication Control Toolkit**.
4. Expand **Server Configuration**.
5. Select **CCT Web Services.**
6. Select the **Enable CCT Web Services** check box.
7. Select the **TLS Security** check box.
8. In the **CA Alias** box, type an alias to identify the CA certificate, such as SomeCAPublicCert1.

9. Click **Import Trusted CA Certificate** to select the CA public certificate.
10. Click **Import Certificate** to select the certificate.
11. Click **Apply Changes**, and then click **OK**.

Configuring SOA CCT Web services

Before you begin

- Understand the network requirements for your installation of Communication Control Toolkit (co-resident, stand-alone, or multimedia).
- Know how to stop and restart the core Communication Control Toolkit services.
- Install and commission Contact Center Manager Server. See *Avaya Aura® Contact Center Installation* (NN44400-311) and *Avaya Aura® Contact Center Commissioning* (NN44400-312).
- Ensure that a valid SOA Web Services (Open Queue and Open Networking) license is available. For more information about configuring licensing, see Enabling Open Queue on page 35.
- If you enable TLS, understand Certificate Authorities, certificate signing requests, and certificates. A Certificate Authority is required to generate the certificates. Configure the SOA Configuration of Certificates using the procedure in Generating a Certificate Signing Request on page 486.

About this task

Configure and enable the SOA CCT Web Services.

Procedure

1. Log on to the Contact Center Manager Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
3. In the left pane of the CCT console, expand **Communication Control Toolkit**.
4. Expand **Server Configuration**.
5. Select **CCT Web Services**.
6. Select the **Enable CCT Web Services** check box.
7. Ensure the **Host Name** box contains the host name of the server.
8. In the **Ports** box, type an available port number where the services are available for access.

9. In the **Domain Authentication Server** box, type the fully qualified domain name of the active directory server that any domain users are to be authenticated against.
10. Select the required **Domain Authentication Method**.
11. In the **Session Timeout** box, select the value of the timeout duration in minutes.
12. To publish services under TLS (HTTPS), select the **TLS Security** check box. To publish services under HTTP, clear the **TLS Security** check box.
13. Click **Apply**.
14. Click **OK**.
15. Stop and restart the core Communication Control Toolkit services.
16. Verify that the services are available by viewing the following on the host: http://localhost:9090.

Variable definitions

Name	Description
Authentication Server	The name of the active directory server that domain users must be authenticated against. The name must be in the format host.domain. For example, myDomainServer.myDomain.com.
Domain Authentication Method	The Domain Authentication Method: Simple or Digest-MD5 specifies if LDAP authentication requests to the Authentication Server is in digest or plain text format. Digest authentication works only with an Active Directory server if the user details are stored with reverse encryption enabled.
Host	The host name of the server, not the IP address.
Port	The port number on which the SOA CCT Interfaces are published. This port, along with the following three consecutive port numbers are used to access the Web services from the external applications. All four port numbers must be available.
Session Timeout	The amount of time in minutes that a session is valid after a user logs on The session times out if it is inactive for the specified duration. The default is 120 minutes.

Name	Description
TLS	To publish services under TLS (HTTPS), select the TLS check box. To publish services under HTTP, clear the TLS check box.

Removing Certificate Configuration

Before you begin

- Clear the TLS Security check box.
- Ensure the certificates are generated. For more information, see Generating a Certificate Signing Request on page 486.

About this task

Remove certificate configuration to delete all imported certificates and any outstanding CSR files.

Procedure

1. Log on to the Contact Center Manager Server.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Communication Control Toolkit** > **CCT Console**.
3. In the left pane of the CCT console, expand **Communication Control Toolkit**.
4. Expand **Server Configuration**.
5. Select **CCT Web Services**.
6. Select the **Enabled CCT Web Services** check box.
7. Click **Reset TLS Encryption Configuration**.
8. In the confirmation dialog box, click **Yes**, and then click **Confirm**.
9. Click **OK**.

Chapter 32: Contact center testing

This section describes how to test the contact center to verify correct operation.

Prerequisites

- Complete the commissioning chapters in this document for your server.
- Configure an agent for testing.
- Configure the Orchestration Designer Contact Router.

Verifying correct operation

About this task

Verify correct operation to ensure your contact center is correctly configured.

Procedure

1. Ensure an agent desk phone is online.
2. Log the agent on.
3. Start the Agent Desktop.
4. Log an Agent into Agent Desktop.
5. Direct a voice call towards the system.
6. Ensure that the call is treated correctly as specified by the TFE script (for example, Ringback, Music on Hold, or IVR) and that the call is routed to the agent.
7. If your contact center supports Instant Messaging, direct an instant message (IM) towards the system.
8. Ensure the IM is treated correctly as specified by the TFE script (for example, automated IM prompts, IM IVR, URL push) and is routed to the agent.

Chapter 33: Common procedures

This chapter describes the common procedures that you use when you commission your Avaya Aura® Contact Center software.

Stopping individual services

Before you begin

- Ensure that you know which server you are working on.
- Ensure that you know which service or services to stop.

About this task

During some procedures, you must stop one or more Windows services to manipulate a feature or function.

Procedure

1. Click **Start** > **Administrative Tools** > **Services**.
2. In the Services window, right-click the name of the service and click **Stop**.

Starting services

Before you begin

- Ensure that you know which server you are working on.
- Ensure that you know which service or services to start.

About this task

During some procedures, you must start one or more Windows services to manipulate a feature or function.

Procedure

1. Click **Start** > **Administrative Tools** > **Services**.

2. In the Services window, right-click the name of the service and click **Start**.

Disabling services

Before you begin

- Ensure that you know which server you are working on.
- Ensure that you know which service or services to disable.

About this task

During some procedures, you must disable one or more Windows services to manipulate a feature or function.

Procedure

1. Click **Start** > **Administrative Tools** > **Services**.
2. In the Services window, right-click the name of the service.
3. Click **Properties**.
4. On the **General** tab, from the **Startup type** list, choose **Disabled**.
5. Click **OK**.
6. Restart the computer.

Enabling services

Before you begin

- Ensure that you know which server you are working on.
- Ensure that you know which service or services to enable.

About this task

During some procedures, you must enable one or more Windows services to manipulate a feature or function.

Procedure

1. Click **Start** > **Administrative Tools** > **Services**.
2. In the Services window, right-click the name of the service.

3. Click **Properties**.
4. On the **General** tab, from the **Startup type** list, choose **Manual** or **Automatic/ Automatic (Delayed Start)**.
5. Click **OK**.
6. Restart the computer.

Stopping and restarting the core Communication Control Toolkit services

Before you begin

- Install Communication Control Toolkit.

About this task

Stop and restart the core Communication Control Toolkit services during CCT console configuration to reset the settings.

Procedure

1. Log on to the Communication Control Toolkit server as Administrator.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**.
3. Select the **CCT** check box.
4. Ensure the check boxes for other installed applications are cleared.
5. Click **Shutdown Contact Center** to make CCT services stop.
6. Click **Yes**.
7. Click **Start Contact Center** after the CCT Status Shutdown is complete.
8. Click **Yes**.

Stopping and restarting the Contact Center Manager Server services

Before you begin

- Install Contact Center Manager Server.

About this task

Stop and restart the Contact Center Manager Server services to reset the settings.

Procedure

1. Log on to the Contact Center Manager Server as Administrator.
2. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**.
3. Select the **CCMS** check box.
4. Ensure the check boxes for any other installed applications are cleared.
5. Click **Shutdown Contact Center** to make CCMS services stop.
6. Click **Yes**.
7. Click **Start Contact Center** after the CCMS Status Shutdown is complete.
8. Click **Yes**.

Adding a server to a domain

Before you begin

- Ensure that you have domain administrator privileges, or ask the Domain Administrator to assign you a domain user account for remote access.

About this task

Add a server to an existing domain. Avaya recommends that you add the server to the domain before installing Contact Center software.

You can change the name of a Contact Center server, but because this is time consuming, Avaya recommends that you consider and configure the server final production name before installing Contact Center software.

Ask your System Administrator to add a Domain Name System (DNS) static entry for this server. Each Contact Center server in a domain requires a DNS static entry.

Important:

Avaya Aura® Contact Center High Availability solutions do not support Windows Server 2008 Dynamic DNS.

In High Availability solutions, ask your System Administrator to add one DNS static entry for the each managed name and associated managed IP address. A typical High Availability campus solution with a pair of co-resident servers requires 3 DNS static entries; one DNS static entry for the active server, one DNS static entry for the standby server, and one DNS static entry for the managed name and associated IP address.

Procedure

1. Log on to the server.
2. Click **Start** > **Administrative Tools** > **Server Manager**.
3. Beside **Computer Information**, click **Change System Properties**.
4. In the **System Properties** dialog box, click the **Computer Name** tab.
5. Click **Change**.
6. In the **Computer Name/Domain 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**.
9. Type your **User name** and **Password**.
10. Click **OK**.
11. Restart the server when you are prompted to do so.

Starting the Contact Center

About this task

The System Control and Monitor Utility (SCMU) enables the administrator to start and stop the contact center applications, for example CCMS and CCT. This procedure describes how to start the contact center.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**.

2. On the Contact Center tab click **Start Contact Center**.
3. Click **Yes**.
4. Select the CCMS and CCT tab to view the started services.
5. Select **Close**.

Important:

If a CCMS monitored service is stopped using the SCMU utility or the Windows Service Control Manager, the CCMS Service monitor cannot restart the service and does not trigger a switchover. This rule permits the administrator to stop a service for maintenance.

Shutting down the Contact Center

About this task

The System Control and Monitor Utility (SCMU) enables the administrator to start and stop the contact center applications, for example CCMS and CCT. This procedure describes how to stop the contact center.

Procedure

1. Click **Start** > **All Programs** > **Avaya** > **Contact Center** > **Common Utilities** > **System Control and Monitor Utility**.
2. On the Contact Center tab, click **Shutdown Contact Center**.
3. Click **Yes**.
4. Select the CCMS and CCT tab to view the stopped services.
5. Select **Close**.

Index

A

about campus critical high availability 361
about integrated reporting 467
about mission critical high availability 305
access remote operating system 37
Active Server 426, 441
active server database backups 321, 348, 377, 406
active server database CCMM 428, 443
active server e-mail 317, 345, 373, 402
active server high availability 314, 343, 370, 401
active server service monitoring 319, 346, 374, 404
active server start 331, 356, 387, 415, 431, 448
active server verifying high availability 333, 358
active server verifying shadowing 390, 417, 432, 449
ActiveX controls 208
adding AML agents 231
adding CCMS servers to CCMA 149
adding CCT to CCMA 216, 225
adding multimedia servers to CCMA 242
adding server to a domain 496
admin users configuring backup server 195
admin users for UCM 188
administration for CCMM 423, 438
Administration user password 144
Agent Desktop client Citrix popups 259
Agent Desktop client commissioning 257
Agent Desktop client hotdesking 259
agent desktop display parameters 134
Agent Desktop standby CCT server 311, 367
Agent Desktop voice contacts LDAP 247
Agent Greeting 16
agent roaming in Contact Center 234
agent roaming in Knowledge worker 464
AML agents adding in CCMA 231
Application Enablement Services default certificates .15
assigning resources 232, 463
attachment e-mail locations 251
availability of servers campus 361
availability of servers critical 305
Avaya Media server statistics 467
Avaya Media Server updates 15
Avaya Mentor videos 20

B

backing up CCMM active server database 428, 443
backup admin user configuration 195
backup communication between CCMA and UCM . .198

C

Call Force Answer Zip Tone 78
    configuring 78
call recording for SIP 485
campus critical high availability about 361
CCMA account shared folders 133
CCMA adding AML agents 231
CCMA adding CCMS servers 149
CCMA adding CCT server 216, 225
CCMA adding multimedia servers 242
CCMA Admin shared folder 133
CCMA admin user for backup 195
CCMA Administration user password 144
CCMA agent desktop display parameters 134
CCMA and UCM communication 190
CCMA backup communication for UCM 198
CCMA certficate signing request 138
CCMA client ActiveX controls 208
CCMA client commissioning 201
CCMA client display settings 203
CCMA client Internet Explorer configuration 203
CCMA client multicast and unicast ports 206
CCMA client port numbers 208
CCMA client shared folders 130
CCMA commissioning 121
CCMA component communication 143
CCMA historical reporting 129
CCMA historical reporting folders 129
CCMA HTTPS security 142
CCMA landing pad configuration 475
CCMA latest documentation 137
CCMA logging on 147
CCMA managed name 335
CCMA real-time reporting 127
CCMA signed certficate installation 140
CCMA starting client 195
CCMA user permissions folders 132
CCMA users mapping UCM users 193
CCMA Web service verification 145
CCMM active server database backup 428, 443
CCMM administration 423, 438
CCMM general administration 445
CCMM server database restore 444

CCMS changing server details 334
CCMS commissioning tasks 33
CCMS configuring multiple sites 44
CCMS confirming services start 42
CCMS contact summary reporting 477
CCMS disk defragmentation 40
CCMS multicast for statistics 40
CCMS multiplicity 36
CCMS open queue 35
CCMS server adding to CCMA 149
CCMS services starting 496
CCMS successful installation verification 35
CCMS verify patches 39
CCT adding to CCMA 216, 225
CCT certification removal 490
CCT commissioning for Contact Center 219
CCT commissioning for knowledge worker 451
CCT confirming services 216, 225, 453
CCT CSR certificates 487
CCT deployment type 214, 223
CCT license 213, 222, 454
CCT open queue configuration 474
CCT server standby 311, 367
CCT services enabling 495
CCT SOA Web services 488
CCT Web Administration 455
CCT windows users 461
CCT workstations 228, 462
certifcates for CCT CSR 487
certificate removal 483
certificate signing request 486
certificate signing requests 479
certificates importing 480
changing server details in CCMS 334
Citrix popups in Agent Desktop 259
client commissioning CCMA 201
client installation Orchestration Designer 155
client starting CCMA 195
clients shared folder 130
commissioning Agent Desktop client 257
commissioning CCMA 121
commissioning CCMS 33
commissioning multimedia 238
commissioning network control center 43
commissioning security framework 185
commissioning SIP-enabled Contact Center server ...21
communication in CCMA 143
communication manager configuring 188
Communication Server 1000 configuring 226, 456
Communication Server 1000 data import 229, 458
component communication for CCMA 143
configure RGN 445
configuring 78
Call Force Answer Zip Tone 78
configuring Active Server 426, 441
configuring admin user 195
configuring admin users 188
configuring CCMA UCM communication 190
configuring CCMM general administration 423, 438
configuring CCT license 213, 222, 454
configuring certificate signing request 479
configuring communication to backup UCM 198
configuring contact summary reporting 477
configuring CS1000 .....226, 456
configuring database backups on active server 321, 348, 377, 406
configuring deployment type 214, 223
configuring desktop display parameters 134
configuring display settings 203
configuring domain accounts 129
configuring e-mail attachment file locations 251
configuring e-mail on active server 317, 345, 373, 402
configuring e-mail recipient addresses 249
configuring high availability on active server 314, 343, 370, 401
configuring high availability on remote geographic server 355, 414
configuring high availability on standby server ..328, 385
configuring hotdesking 234, 464
configuring integrated reporting server 472
configuring Internet Explorer 203
configuring Internet Explorer on the CCMA server ...145
configuring landing pads 475
configuring LDAP for voice contacts 247
configuring license 470
configuring license manager service 126
configuring MIME types 255
configuring multimedia license type 248
configuring multimedia server settings 245
configuring multimedia users 240
configuring open networking Web service 471
configuring open queue 474
configuring real-time reporting 127
configuring remote access 37
configuring server details on remote geographic server 351, 409
configuring server details on standby server 325, 380
configuring service monitoring on active server 319, 346, 374, 404
configuring shared folders for CCMA Admin 133
configuring shared folders for client 130
configuring shared folders for IUSR_SWC 133

configuring shared folders to export historical reports 129
configuring shared folders to read from users 132
configuring SIP call recording 485
configuring sites 44
configuring skillsets 253
configuring SOA CCT Web services 488
configuring SOA Web service 481
configuring workgroup servers 187
confirming CCMS services start 42
confirming services 216, 225, 453
Contact Center agent roaming 234
Contact center assigning resources 232
Contact Center commissioning 21
Contact Center commissioning task 27
Contact Center CS1000 configuration 226
Contact Center CS1000 data import 229
contact center starting 497
contact center stopping 498
contact center virification 235
contact summary reporting 477
coordinating CCMA and CCMS servers 149
creating certificate signing requests 138
creating UCM local accounts 192
critical high availability 305, 361
CS1000 data import for Contact Center 229
CS1000 data import for Knowledge Worker 458
CSR certificates 480
customizing 79
zip tone 79

D

database backups on active server 321, 348, 377, 406
database installation verification 241
database restore 444
database restore on remote geographic server 349, 407
database restore on standby server 323, 378, 429
date and time disabling 38
daylight savings time changes 38
deleting CCT certificates 490
deleting certificate 483
deployment type 214, 223
desktop display parameter configuration 134
disabling date and time features 38
disabling services 494
disabling Windows time 38
disk defragmentation 40
display settings configuration in CCMA client 203
documentation downloads 137
domain adding server 496
downloading documentation 137

E

e-mail attachment locations 251
e-mail on active server 317, 345, 373, 402
e-mail recipient addresses 249
enabling CCT services 495
enabling component communication 143
enabling HTTPS security 142
enabling multiplicity 36
enabling open queue 35
enabling services 494
exceptions list for IE firewall 206
Explorer ActiveX controls 209
Explorer on CCMA client 203

F

firewall exceptions 206
first log on to CCMA 147
FQDN configuring workgroups 187

G

generating certificate signing request 486
geographic remote server details 351, 409
geographic remote server high availiability 355, 414
geographic remote server restore 349, 407
geographic remote server shadowing 357, 416, 449

H

High Availability CCMM 425, 440
high availability on active server 314, 343, 370, 401
high availability on geographically remote server 355, 414
high availability on standby server 328, 385
High Availability RGN CCMM 446
high availability switchover testing 336
high availability third-party support 313, 342, 369, 400, 423, 438
high availability verification 342, 400
high availability verification on active server 333, 358
high availability verifying services 313, 369
historical reporting domains 129
historical reporting shared folder 129
hotdesking for Agent Desktop client 259
hotdesking in Contact Center 234
hotdesking in Knowledge worker 464
HTTPS security for CCMA 142

I

importing CS1000 data 229, 458
importing CSR certificates 480
importing Windows users from CCT 461
importing workstations from CCT 228, 462
individual services stopping 493
inporting CCT CSR certificates 487
installation CCMS verification 35
installing Orchestration Designer client 155
installing signed certificate 140
installing third-party utilities for HA 313, 342, 369, 400, 423, 438
integrated reporting about 467
integrated reporting server configuration 472
Internet Explorer Active X controls 209
Internet Explorer firewall exceptions list 206
Internet Explorer on CCMA client 203
IP addresses managed for high availability 312, 368
IUSR_SWC shared folder 133

K

Knowledge worker agent roaming 464
Knowledge worker assigning resources 463
Knowledge Worker CCT Web administration application 455
Knowledge Worker CS1000 configuration 456
Knowledge Worker CS1000 data import 458
Knowledge worker verification 465

L

landing pad configuration 475
latest documentation 137
LDAP server for AAAD voice contacts 247
license manager configuration 126
licensing 470
licensing for multimedia 248
licensing in CCT 213, 222, 454
local multimedia users permissions 240
local UCM accounts 192
logging on privileges for multimedia 240
logging on to CCMA 147

M

managed IP addresses 312, 368
managed name for CCMA 335
mapping UCM users to CCMA 193
mission critical high availability about 305
multicast controller 40
multicast ports 206
multimedia Citrix popups 259
multimedia commissioning 238
multimedia database installation 241
multimedia e-mail attachment locations 251
multimedia e-mail recipient addresses 249
multimedia hotdesking 259
multimedia in CCT 214, 223
multimedia LDAP server 247
multimedia license types 248
multimedia MIME types 255
multimedia server settings 245
multimedia servers to CCMA adding 242
multimedia services start 241
multimedia skillsets 253
multimedia users configuring 240
multiplicity enabling 36

N

name managed for high availability 312, 368
network addressing for statistics 40
network control center commissioning 43
networking configuring sites 44
Networking Web service 471
numbers for ports in CCMA client 208

O

observe and barge-in tones 77
Open Networking feature license 470
open networking SOA Web service 481
open networking Web service 471
open queue configuration 474
open queue enabling 35
open queue SOA Web service 481
operating system remote access 37
optimizing performance 40
Orchestration Designer installation 155

P

passwords for CCMA Administration users 144
patches CCMS verification 39
port numbers 208
ports in CCMA client 206
Presence Services server for instant messaging 16

R

read permissions for clients in shared folder configuration 130
real-time data multicast 40
real-time reporting 127
recipient addresses 249
Reference Client in Contact Center 235
Reference Client in Knowledge worker 465
related resources 20
Avaya Mentor videos 20
remote access for operating system 37
remote geographic server database restore 349, 407
remote geographic server details 351, 409
remote geographic server high availability 355, 414
remote geographic server shadowing 357, 416, 449
removing CCT certificate configuration 490
removing certificate 483
reporting contact summary data 477
reporting historical configuration 129
reporting historical shared folder configuration 129
reporting real-time data configuration 127
reporting server integration 472
requests for signing certificates 138, 479
resolving managed names 312, 368
resources in Contact Center 232
resources in Knowledge worker 463
restoring database 444
restoring database on remote geographic server 349, 407
restoring database on standby server 323, 378, 429

S

scheduling disk defragmentation 40
scheduling historical reports 129
security for HTTPS in CCMA 142
security framework commissioning 185
server adding to a domain 496
server CCT Agent Desktop standby 311, 367
server details in CCMA 334
server details on remote geographic server 351, 409
server details on standby server 325, 380
server settings for multimedia 245
servers campus availability 361
servers coordinating CCMA and CCMS 149
servers critical availability 305
service monitoring on active server 319, 346, 374, 404
service provider for Contact Center 226
service provider for Knowledge Worker 456
services availability for high availability 313, 369
services disabling 494
services enabling 494
services enabling CCT 495
services for CCMS confirming 42
services for multimedia 241
services restarting CCMS 496
services starting 493
services starting in CCT 216, 225, 453
services stopping 493
shadowing on remote geographic server 357, 416, 449
shadowing on standby server 332, 388, 431
shadowing verification on active server 390, 417, 432, 449
shared folders for clients to read 130
shared folders for historical reporting 129
shared folders for IUSR_SWC and CCMA Admin 133
shared folders for user permissions 132
signed certificate installation 140
signing certificate request 138
signing request 486
SIP call recording 485
SIP Contact Center server commissioning 21
site configuration 44
skillsets 253
SOA CCT Web services 488
standby CCT server 311, 367
standby server database restore 323, 378, 429
standby server high availability 328, 385
standby server server details 325, 380
standby server shadowing 332, 388, 431
starting active server 331, 356, 387, 415, 431, 448
starting CCMA client 195
starting CCMS services 496
starting CCT Web Administration 455
starting contact center 497
starting services 493
starting shadowing on remote geographic node server 357, 416, 449
starting shadowing on standby server 332, 388, 431
statistics Avaya Media server 467
stopping contact center 498
stopping services 493
support 19
contact 19
switchover testing 336

T

tasks for Contact Center commissioning 27
testing switch overs 336
third-party support for high availability 313, 342, 369, 400, 423, 438
time and date disabling 38
time disabling in Windows 38

tones 77
silencing observe and barge-in 77

U

UCM and CCMA communication 190
UCM backup communication 198
UCM configuration 188
UCM local account creation 192
UCM mapping to CCMA users 193
unicast ports 206
updating CCMA Administration password 144
user accounts shared folder configuration 133
user mapping from UCM to CCMA 193
user permissions shared folder 132
user permissions shared folder configuration 132
users Administration password 144
users for UCM 188
users for Windows in CCT domain 461
using CCMA managed name 335

V

verifying CCMS installation 35
verifying CCMS patches 39
verifying CCT Contact Center 235
verifying CCT Knowledge worker 465
verifying high availability 342, 400
verifying high availability on active server 333, 358
verifying multimedia database 241
verifying multimedia services 241
verifying services for HA 313, 369
verifying shadowing on active server . 390, 417, 432, 449
verifying Web services in CCMA 145
videos 20
Avaya Mentor 20

W

Web administration for CCT Knowledge worker 455
Web browser ActiveX controls 208
Web service Open Networking 471
Web service SOA Open Networking 481
Web service SOA Open Queue 481
Web services in CCMA 145
Windows time disabling 38
Windows users in CCT domain 461
Windows XP port numbers 208
workgroup server configuration 187
workstations domain 228, 462

Z

zip tone 79
customize 79